Physical-layer identification of wireless sensor nodes

Physical-layer Identification of Wireless Sensor Nodes

Boris Danev
System Security Group
ETH Zurich, Switzerland
bdanev@inf.ethz.ch

Srdjan Capkun
System Security Group
ETH Zurich, Switzerland
capkuns@inf.ethz.ch

ABSTRACT

Identification of wireless sensor nodes based on the physical characteristics of their radio transmissions can potentially provide additional layer of security in all-wireless multi-hop sensor networks. Reliable identification can be means for detection and/or prevention of wormhole, Sybil and replication attacks, and for complementing cryptographic message authentication protocols. In this paper, we propose an improved method for capturing and analysis of sensor node radio signals for reliable and accurate recognition. We investigate the performance accuracy of our approach in terms of parameters such as distance, antenna polarization, voltage and show that it achieves recognition with EER=0.24%. We also propose and perform practical attacks on the recognition to further evaluate the robustness of the proposed method under security threats.

1. INTRODUCTION

Identification of components in a networked environment (e.g., operating systems, drivers, physical device) can benefit a number of applications such as authorized access, forensics, device cloning and malfunctioning detection, inventory management, tracking. It is commonly referred to as fingerprinting i.e., determining a specific characteristic (*fingerprint*) of a network device component with or without its cooperation.

In a typical scenario, the *fingerprinter* observes or creates specialized traffic to and from a targeted device (*fingerprintee*) in order to find unique characteristics that uniquely distinguish a component of the device or the whole device. Fingerprinting spans physical [1, 2, 3], link [4, 5] and network/application [6] layers for a variety of purposes such as identifying the type of a device [4], operating system [7, 8], particular drivers [5] or the physical device itself [1, 2, 3, 6].

In this work, we focus on physical device recognition (verification) of wireless sensor nodes by distinguishing characteristics of the radio signals transmitted by these devices. This approach is commonly referred to as radio frequency fingerprinting (RFF). Unlike device unique identifiers such as IDs and MAC addresses, device RFFs cannot be simply modified by their users. RFF forging typically requires modification of the device hardware and is challenging even for attackers with access to sophisticated instrumentation.

What motivates this work is that physical device recognition based on RFF can enhances the security of all-wireless sensor networks [9]. It can enable detection and/or prevention of wormhole [10], Sybil [11] and replication [12] attacks. Additionally, it can be used to complement cryptographic message authentication protocols in order to ensure an additional layer of security against key compromise.

Prior work on RFF of sensor nodes reported sensor signal classification accuracy of 70% from $\leq$15 cm distance [9]. In this work, we show that identical (i.e., same manufacturer, same model and same hardware) sensor nodes can be recognized from larger distances (tested up to 40 m indoors) with a much higher accuracy - Equal Error Rate (EER) = 0.24%.

For this purpose, we propose an improved signal capturing method and related spectral DFT-based fisher-features for sensor node identification. Our method enables highly accurate sensor node recognition from short and longer distances. We further analyze the recognition accuracy in terms of number of signals used for feature extraction, distance, antenna polarization, voltage and temperature. We quantify the trade-offs by means of EER and Receiver Operating Characteristic (ROC), the most agreed way to evaluate recognition systems [13, 14].

Furthermore, we design and perform various attacks. We show that a hill-climbing attack for device impersonation make the recognition system highly vulnerable when the number of signals used for recognition is small. We also demonstrate that a denial-of-service jamming attack prevents accurate recognition and discuss the requirements for a number of other attacks that can potentially compromise the identification.

The remainder of this paper is organized as follows: In Section 2, we present our signal capturing process and describe the proposed features for sensor node recognition. In Section 3, we analyze the recognition accuracy of our approach. In Section 4, we develop a num-

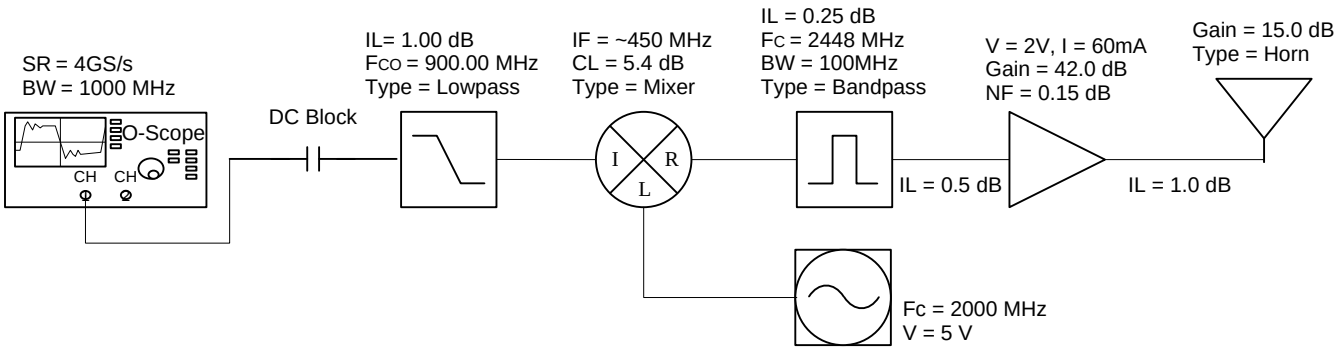

Figure 1: Radio signal capturing hardware setup.

ber of attacks and discuss their outcomes. We describe possible applications in Section 5, give background and related work in Section 6 and conclude the paper in Section 7.

2. SPECTRAL FISHERFEATURES FOR SENSOR NODE RECOGNITION

In this section, we first describe the hardware components used to accurately capture the radio signal and motivate the choice of the selected components based on different experimentations. We then detail our proposed feature extraction and matching methods.

2.1 Signal Capturing Process

Figure 1 displays the hardware components that we used for signal capturing. The signal is first captured by a Standard Horn directional antenna and subsequently amplified by an ultra low-noise and low power amplifier (NF=0.15 dB). Due to the low power of the sensor devices, it is critical to amplify the signal without loosing discriminant capabilities, as the signal-to-noise ratio (SNR) degrades drastically within couple of meters. An ultra low-noise and low-power amplifier proved to be the best choice among a number of amplifiers we have tested.

An ultra low-insertion loss bandpass filter is used to eliminate radio frequencies outside the IEEE 802.15.4 band [15]. The amplified and filtered radio signal is then down-mixed to an intermediate frequency of 450 MHz using a standard frequency mixer and a voltage controlled oscillator(VCO). This procedure is also critical for achieving accurate recognition from a distance. 2.4 GHz signals can only be captured accurately by high bandwidth oscilloscopes ($\geq$5 GHz) which cost between 100-150 K. Our 1 GHz oscilloscope significantly attenuated the high frequencies of signals (-25db), which degraded the recognition accuracy. We opted for 450 MHz as intermediate frequency as it allowed to capture the signals with sufficient precision (i.e., number of harmonics). This solution proved to provide competitive recognition accuracy (see Section 3).

Due to frequency artifacts in down-mixing process, the intermediate frequency signal is passed through a lowpass filter and a DC blocking capacitor before it is recorded on a our 1 GHz bandwidth, 4 GS/s sampling rate oscilloscope[1].

Our capturing setup was designed on purpose with off-the-shelf small-size components. Therefore, it can be integrated with compact data acquisition boards with standard FPGA and sampling rate of 1-2 GS/s. These boards are sufficient to accurately represent the 450 MHz signals. It is even possible to build the setup in a printed-circuited board (PCB) by using surface mount components instead of the currently used coaxial ones. We acknowledge that the price of such boards is currently high (7-10 K). Therefore more investigation is needed to see if lower intermediate frequencies also preserve sufficient discriminant information in the transient part of the signal. This could significantly reduce the price for building the device.

2.2 Spectral Fisherfeature Extraction

In feature extraction, spectral fisherfeatures are extracted using a linear transformation derived from Linear Discriminant Analysis (LDA). Fig. 2 illustrates the proposed scheme for the extraction process and matching using the features.

First, we extract the transient part of the recorded signal l by using a threshold detection algorithm [9]. We denote this extracted signal by $f(t,l)$ (see Fig. 2), where $f(t,l)$ is the amplitude of the transient of signal l at time t. Subsequently, we apply the one-dimensional Fourier transformation to $f(t,l)$ (step (i) on Fig. 2):

$$F(\omega,l) = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} f(t,l) \exp(-2\pi i \frac{t\omega}{M}) \quad (1)$$

where $0 \leq t \leq M-1$, M - transient length

Second, a projected vector $\vec{g_l}$, also called a fisherfea-

[1]Additional optimization was to utilize high quality SMA cables with low insertion loss (approximately 0.5 dB depending on the cable length used). First experimentations with standard BNC precision cables highly attenuated the signal.

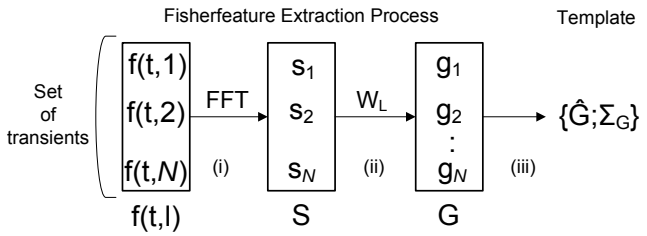

Figure 2: Feature extraction process.

ture, is extracted from the Fourier spectrum using an LDA matrix W_L (step (ii) on Fig. 2):

$$\vec{g_l} = W_L^t \vec{s_l} \tag{2}$$

Here, $\vec{s_l}$ denotes the relative differences between adjacent spectra of the $|F(\omega, l)|$ in a vector form: $\vec{s_l} = [\ |F(2,l)| - |F(1,l)|\ |F(3,l)| - |F(2,l)|\ \cdots\ |F(M/2-1,l)| - |F(M/2-2,l)|\ ]^t$ where the DC component and redundant half of the spectrum are removed.

Based on the above description, the fisherfeature extraction from a set of signals is written as $G = W_L^t S$ where G is an array of g_l, S is a matrix $S = [\ s_0\ ..\ s_l\ ..\ s_N\ ]$ and N is the number of radio signals in the set. Finally, the feature template $\boldsymbol{h}$ used for matching (recognition) becomes (step (iii) on Fig. 2):

$$\boldsymbol{h} = \{\hat{G}; \Sigma_G\} \tag{3}$$

where $\hat{G}$ denotes the mean vector of G and Σ_G denotes the covariance matrix of G. The set size N and the number of projected vectors in W_L (i.e., the Fisher subspace dimension) are experimentally determined.

2.3 Training and Mahalanobis Matching

The LDA matrix W_L is derived by a standard LDA procedure based on scatter matrices [16]. The W_L is the optimal Fisher discriminant projection given as the set of κ eigenvectors in matrix W corresponding to the κ-highest eigenvalues in the generalized eigenvalue problem: $S_b W = \Lambda S_w W$ where Λ is the eigenvalue matrix, S_w is the within-class scatter matrix showing the average scatter of sample features $\boldsymbol{h}$ from the same sensor device and S_b is the between-class scatter representing the average scatter of sample features $\boldsymbol{h}$ from different sensor devices.

Mahalanobis distance is used to find the similarity score between the feature templates. A reference and test feature templates $\boldsymbol{h}^R$, $\boldsymbol{h}^T$ are matched as follows:

$$Score = \sqrt{(\boldsymbol{h}^T - \boldsymbol{h}^R)^t \Sigma_G^{-1} (\boldsymbol{h}^T - \boldsymbol{h}^R)} \tag{4}$$

It should be noted that the proposed feature extraction and matching method can be efficiently implemented in hardware as it uses only linear transformations for feature extraction and inter-vector distance matching to compute similarity. These operations have a low memory footprint and are computationally very efficient.

3. PERFORMANCE EVALUATION

In this section, we evaluate the recognition accuracy of our method. We first present the parameters of our investigation and the methodology used for evaluation. We then describe the data acquisition, data characteristics and experimental results.

3.1 Parameters of Investigation

To assess the practicality of physical-layer identification for intrusion detection, replay protection, message authentication and device tracking, we address a variety of interrelated questions:

1. What recognition accuracy can be achieved for COTS wireless sensor devices?
2. How is the recognition accuracy affected by the number of radio signals used for recognition and distance of the device from the fingerprinter?
3. What are the effects on recognition accuracy in terms of factors such as antenna polarization, voltage and temperature?
4. Do techniques to attack physical-layer identification (e.g., impersonate a sensor device) without "exactly" cloning the hardware circuitry exist?

Answers to the above questions will help to identify the type of applications our proposed identification method is suitable for.

3.2 Recognition Model

A physical device recognition system typically can work in two modes, either identification of one device from among many, or verification that a device's physical signature (fingerprint) matches its claimed identity [13]. Positive identification determines that a given device is in a (member) database; functionally it is the same as verification. Negative identification is determining if a device is not in some negative list of devices.

In this paper, we consider positive identification and more precisely verification of a device's claimed (assumed) identity. The verification procedure matches the physical signature of a device based on its claimed or assumed identity and provides an Accept/Reject decision based on a threshold value. It can be achieved by a special device (centralized approach) or in each device itself (distributed approach). Verification requires "1:1" signature comparison and is therefore applicable (scalable) in security applications for large wireless sensor networks (see Section 5).

3.3 Methodology

We adopt Equal Error Rate (EER) and Receiver Operating Characteristic (ROC) for evaluating the recognition accuracy of our proposed method since these are

Table 1: Data acquisition sets.

Set	Goal	Dist.	# Signals	# Nodes	Total
1	Accu.	10 m	600	50	30000
2	Accu.	40 m	600	10	6000
3	Volt.	10 m	200	10	2000
4	Polar.	-	600	10	6000
5	Attack	10 m	350	3	1050

the most agreed and correct ways for evaluating identification systems [13]. Here we briefly summarize the main concepts and measures used for our evaluation.

Given two samples, if we consider the *null* hypothesis H_o - the two samples match and the *alternative* hypothesis H_a - the two samples do not match, we can construct the two possible errors False Accept and False Reject as follows:

- *False Accept*: Decide H_o when H_a is true, is equivalent to decide that a device (claimed) identity is a legitimate one while in reality it is an imposter;
- *False Reject*: Decide H_a when H_o is true, is equivalent to decide that a device identity is not a legitimate one while in reality it is;

Based on these two errors, evaluating our system reduces to compute the *False Accept Rate (FAR)* and the *False Reject Rate (FRR)*, the frequencies at which these errors occur. The FAR and FRR are tightly related to each other. They show the trade-offs of operation of a recognition system in the Receiver Operating Characteristic (ROC). The ROC is a curve where if one fixes the desired probability of False Accepts for operation, then the False Rejects can be automatically computed, and vice versa [13]. In this paper, we used the *Genuine Accept Rate* (GAR = 1 - FRR) instead of FRR for displaying the ROC because it shows the rate of accepts (instead of rejects) of legitimate identities.

The operating point in ROC where FAR and FRR are equal is the *Equal Error Rate* (EER). The EER represents the most common measure of the accuracy of a recognition system [14]. Therefore, in our evaluation, we use primarily EER and ROC to evaluate the recognition accuracy. Where appropriate, we also calculate FRR for fixed values of FAR.

3.4 Data Acquisition

Using the signal capturing setup described in Section 2.1, we collected data for analysis of the different parameters of investigation outlined in Section 3.1. The recorded datasets and main measurement parameters are summarized in Table 1.

Our population (P) of devices consisted of 50 COTS Tmote Sky sensor nodes with manufacturer signature "4M 94V-0 H014-4787" (i.e., same manufacturer, same model and same hardware specification). Given that they were purchased in separate sets, we cannot fully assert that they were all produced from the same production line, even though such an assumption is highly plausible.

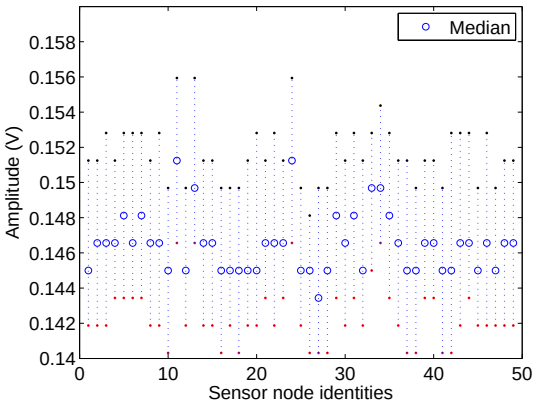

Figure 3: Inter/intra maximum amplitude variation of the 50 sensor devices.

During data acquisition, each node was positioned on the same tripod, previously fixed at a given distance from the fingerprinter's antenna. The antenna polarization of the sensor device (using the on-board integrated antenna) and of the fingerprinter were the same and perpendicular to the ground. The devices were run on 2 x 1.5V AA batteries (Datasets 1,2,4,5) and 2 x 1.2V AA batteries (Dataset 3). The experiments were made indoors and in an underground parking space (Dataset 2) for about 20 minutes with constantly spaced transmissions in order to acquire a predefined number of samples.

3.4.1 *Inter/intra Maximum Amplitude*

We observed that the maximum amplitude of the captured signals is quite stable (see Fig. 3). The median of the inter maximum amplitude of 90% of the devices was in the range between 145 mV and 148 mV. The intra variation of the signal maximum amplitude (from the same device) also proved stable (approximately $\pm 5\ mV$ around the median value).

The results show that under the same acquisition conditions (distance and antenna polarization) the devices behave in a consistent way.

3.4.2 *Transient Data Samples*

Each acquired sample signal consisted of a 500 ns power trace of which the transient consistently lasted approximately 125 ns for all the nodes in our population set. Given the 4GS/s sampling rate of our oscilloscope, this corresponded to approximately 500 data points. We thus define the transient as 512 data points from its detected starting point; the starting point is determined by the variance-based threshold detection algorithm detailed in [9].

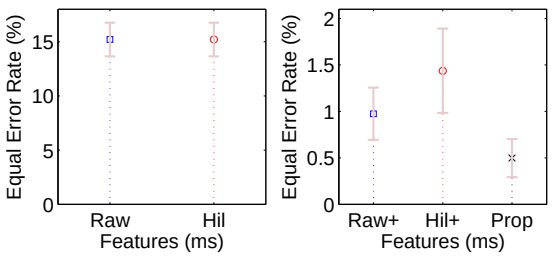

Figure 4: Recognition accuracy of the initial features (P=50, D=10m).

3.5 Recognition Experiments

In the following experiments, we proceeded in evaluating our proposed scheme (Section 2). We first considered Dataset 1 as it contains signals from the full set of sensor nodes (P=50) taken from a 10 m distance (D=10m). We later show that the achieved accuracies are preserved for other datasets (see Table 1).

3.5.1 Initial Feature Selection

The purpose of feature selection is to select the most accurate initial transformation of the transient data samples. We considered the following transient data sample transformations:

- Raw - The original transient data samples are used. No transformation.
- Hil - The envelops of the transient data samples obtained by the Hilbert transformation. This technique was proposed in [17].
- Raw+ - The FFT spectra obtained from the original transient data samples are used.
- Hil+ - The FFT spectra obtained from the envelops of transient data samples are used.
- Prop - the proposed relative differences between adjacent FFT spectra obtained from the original transient data samples are used.

The recognition accuracy (EER) is summarized in Figure 4. The number of signals used to form the test and reference templates was fixed to N=50. This resulted in a total of 300 genuine and 22050 imposter matchings. The confidence intervals were estimated with 4-fold cross validation [16].

The obtained results show that using the original transient data samples or their envelops score a high EER, therefore low recognition accuracy (i.e., allowing 15% of False Accepts, means only 85% of Genuine Accepts). This makes them not suitable as a choice of initial features for further analysis. On the other hand using the Fourier spectra significantly improved the accuracy; our proposed features further improved that accuracy. We therefore chose the proposed relative differences between adjacent FFT spectra as initial features.

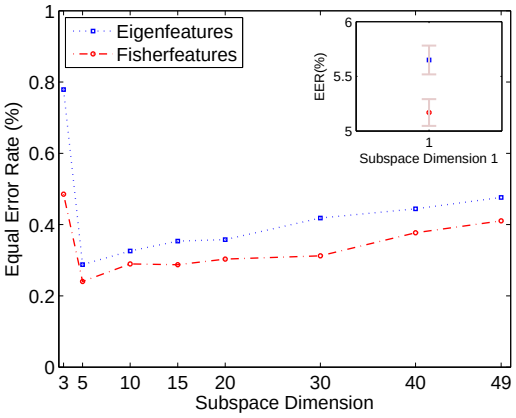

Figure 5: Eigen- vs. Fisher-features accuracy for variable subspace dimension (P=50, D=10m).

3.5.2 Eigen- vs. Fisher-feature Extraction

We compare Eigen- and Fisher-feature extraction from the initial features previously selected for N=50. This is based on PCA and LDA training procedures respectively. We also experimentally select the number of eigenvectors that achieved the highest recognition accuracy. The total dataset per sensor node was split into four folds (4 x 150 transient data samples); three folds were used for training and one fold for testing. This resulted in a total of 300 genuine and 22050 imposter matchings per fold.

Figure 5 shows the EERs achieved by varying the dimension of the linear eigen- and fisher-subspaces. The dimension of the initial features was 254. The Fisher-subspace was more efficient for lower dimensional subspaces (1-3 eigenvectors) compared to the eigenspace. However, we cannot assert with statistical confidence such a behavior for higher dimensional subspaces. Even though the average EERs suggest that, 4-fold cross validation (the maximum possible with N=50) produces quite large (overlapping) confidence intervals. Related work on biometric recognition [18, 19] have shown fisher-features to be more effective and optimal results found in the low dimensional subspaces. We selected the Fisher-subspace with the first 5 eigenvectors for feature representation.

Figure 6 shows the EERs achieved by varying the dimensionality and the number of signals N used to form the reference and test templates. Reducing the number of signals allowed to perform 5-fold cross validation (5 folds x 120 signals) and increased the number of genuine and imposter matchings (see Table 2 for more details).

The results confirm that using the first 5 eigenvectors for projection scored the highest recognition accuracy. The EER degrades progressively in higher dimensional

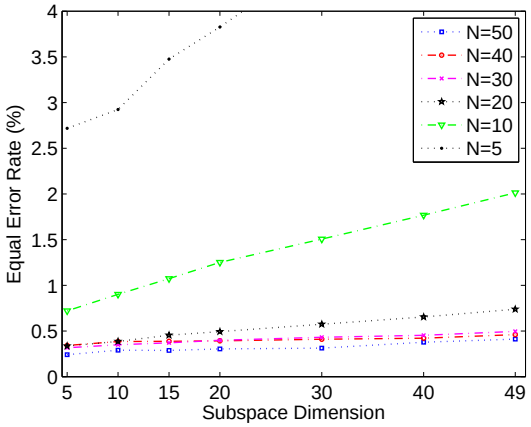

Figure 6: Recognition accuracy for variable dimension and number of signals N (P=50, D=10m).

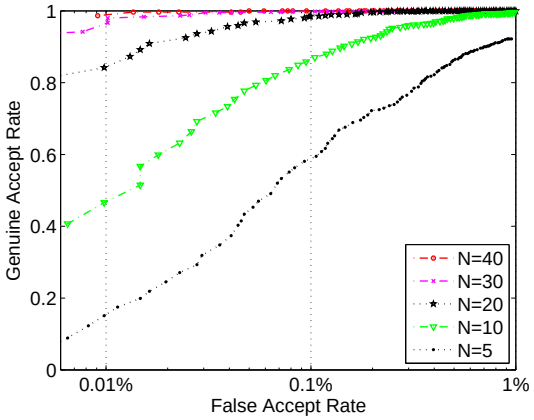

Figure 7: Recognition accuracy with variable number of signals N and fixed 5-dimensional subspace (P=50, D=10m). See Table 2 for the numeric results.

subspaces. This phenomenon is even more pronounced when the number of signals N decreases, in particular for feature templates constructed with 5 and 10 sample signals. The results also demonstrate that our proposed features keep competitive EER even if few signals are used for the feature template construction.

3.5.3 *Summary and ROC*

We demonstrated with a number of experiments the recognition efficiency in terms of Equal Error Rate of our proposed capturing setup and related spectral FFT-based fisherfeatures. We found that a 5-dimensional linear subspace is enough to represent a transient signal for accurate verification. Therefore, our proposed features form very compact and computationally efficient feature templates.

In order to complete the analysis and fully characterize the accuracy trade-offs, we draw the Receiver Operating Characteristic (ROC) with respect to the number of signals N for feature template construction. Figure 7 displays the ROC curves and Table 2 summarizes the main parameters, namely the number of signals N used for the feature template, the total genuine and imposter matchings performed, the FRR for common FAR targets and the EER and its statistical confidence.

An interesting observation is that even if the EERs for feature templates composed of N=10,20,30,40,50 signals were very similar (see Figure 6), using the ROC, we can state that reducing the number of signals degrades the Genuine Accept Rate (GAR = 1 - FRR) for lower False Accept Rates (e.g., FAR = 0.01%). Such analysis shows that if an application requires a very low FAR, it must use more signals to build a feature template for recognition in order to ensure a high GAR.

3.6 Feature Stability

In the following analysis, we investigate the stability of our proposed recognition in terms of distance (i.e., channel attenuation), antenna polarization, voltage and temperature.

3.6.1 *Distance*

For any practical usage of physical-layer recognition, we must consider the effect of channel attenuation. For convenience reasons (e.g., readily available electricity), we performed measurements in the university parking, which allowed us to collect signals from 40 m line-of-sight. We used the first 10 sensor devices from our population set for this purpose (Dataset 3).

Table 3 compares the achieved EERs in terms of the number of signals N for a distance of 10 and 40 m respectively. We can observe similar recognition accuracy. This shows that our capturing setup (Section 2.1) was successful in preserving the discriminant power of the transient part of the signal.

It should be pointed out that for N=50,40,30, the algorithm achieved EER=0.00%. This confirms that the EER must be computed for a larger set of devices in order to have a more accurate estimation of the recognition capabilities. In similar recognition systems (e.g., biometrics), usually hundreds and even thousands different biometric identifiers (e.g., fingerprints, faces) are used for evaluation (e.g., NIST, FERET databases).

Even though all signal capturing was done in a university parking place with numerous possibilities for reflection (e.g., cars, concrete columns, etc), we did not observe multipath propagation problems, i.e. capturing two or more transients at the same time. We acknowledge that such superposition of transients might prevent accurate recognition. Therefore, it needs to be detected and eliminated from the computation of the matching features.

In order to complete the analysis on the effect of dis-

Table 2: Summary of recognition accuracy (P=50, D=10m).

N	Test matchings		Threshold	FRR (%)		EER (%)	Confidence (%)		Validation
	Genuine	Imposter		FAR=0.01%	FAR=0.1%				
50	300	22050	3.01	0.725	0.650	**0.240**	0	0.491	4-fold
40	300	22500	3.95	1.100	0.460	**0.342**	0.023	0.661	5-fold
30	600	39200	3.87	2.920	0.612	**0.317**	0.072	0.560	5-fold
20	1000	61250	4.10	12.94	1.240	**0.336**	0.201	0.469	5-fold
10	1000	61250	6.74	52.00	9.600	**0.720**	0.622	0.817	5-fold
5	1000	61250	16.04	82.12	40.10	**2.718**	2.383	3.051	5-fold

Table 3: Comparison accuracy (P=10).

N	Test matchings		EER (%)		Valid.
	Genuine	Imposter	10 m	40 m	
50	60	22050	0.00	0.00	4-fold
40	60	22500	0.00	0.00	5-fold
30	120	39200	0.00	0.00	5-fold
20	200	61250	0.57	0.36	5-fold
10	200	61250	1.35	3.41	5-fold

tance on the recognition accuracy, we performed cross-matching between features extracted at 10 m and 40 m distance from the capturing antenna. We registered on average a recognition accuracy of EER=38.01% for N=50. Such result shows that while the frequency information in the transient part of the signal is unique within a given distance, it changes across different distances at the same antenna polarization. Variable polarization is discussed in Section 3.6.3.

3.6.2 *Voltage and Temperature*

Given that sensor nodes are generally run on battery supply, we proceeded into evaluating the effect of voltage. For this purpose, we used transient data samples captured with 2x1.5V standard alkaline batteries and transient data samples captured with 2x1.2V NiMH batteries. Thus the difference of supplied voltage was approximately 0.6V.

Figure 8 shows the similarity (matching) score between transient data samples taken at the same voltage level (blue squares) and the similarity score between transient data samples taken at different voltage levels (2.4V and 3V respectively) (red circles). We do not observe a significant difference in similarity score between genuine matchings coming for same and different voltage levels, i.e. the scores are very close to 0 and within the boundary of the genuine score distribution for N=50.

This is an expected result given that the Tmote Sky sensor nodes are equipped with a low power microcontroller. It requires 2.1-3.6V for normal functioning. However, it should be noted that such a result is not necessary true for high power transmitters (e.g., VHF FM) as observed in [20].

Our experiments did not suggest any effect on recognition accuracy from the surrounding temperature changes (indoor air-conditioned environment or non air-conditioned parking place). However, we did not investigate extreme changes of temperature (e.g., intentional heating of the sensor nodes).

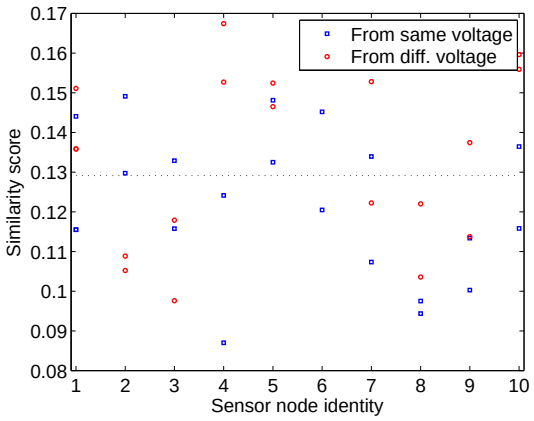

Figure 8: Score matchings with variable voltage: the (blue) squares represent matching scores of features from the same sensor node and same voltage level; the (red) circles represent matching scores of features from the same sensor node at different voltage levels (2.4V and 3V).

3.6.3 *Polarization*

The polarization of an antenna is the polarization of the wave radiated by the antenna. At a given position, the polarization describes the orientation of the electric field. This orientation will change in sensor network applications where the nodes change their position with respect to the receiving antenna. A direct implication is the shape change of the transient part of the signal as shown in Figure 9 for two different orientations.

We first collected transient data samples under the same conditions as in dataset 1 but changing the polarization of the antenna on the sensor node by 45°. We then applied our feature extraction method and matched the transient data samples. This resulted in degrading the recognition accuracy (EER = 39%).

As this could have been influenced by the training procedure where only training data from one type of

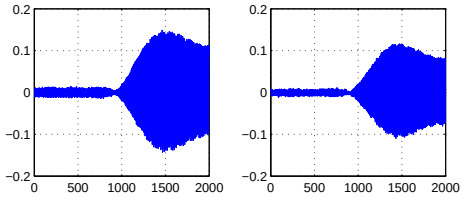

Figure 9: Transient signal shapes from a sensor node at two different antenna polarizations.

polarization was used, we collected transient data samples from 10 sensor nodes from three different antenna polarizations. The recognition accuracy did not improve. This result shows that polarization changes the FFT-based frequency features. These changes can not be well separated by means of a linear kernel (in our case Fisher discriminant). We acknowledge that further work is needed to quantify this change more precisely in order to draw conclusions about how much change in polarization can be tolerated.

3.7 Summary and Comparison

The results show that sensor nodes can be recognized with high accuracy by analyzing the transient part of the transmitted signals. Such recognition proves to be robust to channel attenuation (distance), multipath propagation and voltage changes. As such, it can be effectively used in sensor network applications where the sensor nodes do not often move.

Transient shape changes due to antenna polarization (mobility) introduce variability that degrades the recognition accuracy. This finding limits the usability of only transient-based features in applications where sensor nodes frequently move. However, our features can still be combined with other techniques (e.g, directionality, RSSI) to further reduce the set of probable sensor nodes from which the signals came.

In application scenarios, where the number of sensor devices is known and never changes, classification error rate [16] can be used to evaluate the ability of the fingerprinting approach to classify (map) the transmitted signals to their corresponding devices. Table 4 displays the average classification errors using our proposed features on the full set of 50 nodes for typical 1-NN and 2-NN classifiers.

Comparison of the classification error rates in Table 4 with related work can be misleading given the difference in device population (same vs different manufacturers), device hardware and radio specification, capturing distance, etc. However, our approach outperforms previous work on transient-based identification of identical wireless sensor nodes [9] where classification error was about 30% for an 1-NN classifier. Our results are comparable with [21] where identical wireless devices were also used for evaluation. An advantage of our approach

Table 4: Average classification error rates.

N	# Samples	1-NN (%)	2-NN (%)	Valid.
50	300	0.075	0.00	4-fold
40	300	0.075	0.00	5-fold
30	600	0.25	0.075	5-fold
20	1000	0.975	0.45	5-fold
10	1000	3.7	2.43	5-fold

is that the classification error rate improves when the number of signals used for feature extraction increases reaching 0.075% for N=40,50.

It should be noted that the results also confirm that classification error rate does not accurately assess the recognition accuracy. A very low classification error does not necessarily provide high recognition accuracy (see EER in Table 4 vs Table 2 for N=40,50), and a higher classification error does not either imply low recognition accuracy (see EER in Table 4 vs Table 2 for N=10,20).

It should be noted that the results in Table 4 may be improved by using more sophisticated classifiers (e.g., SVM, PNN). However, they need to be augmented with doubt and outlier classes in order to fit the requirements for recognition. In addition, they are also memory expensive and require significant computational resources, therefore are not suitable for the applications discussed.

4. SECURITY ANALYSIS

In this section, we analyze the robustness of our identification approach to impersonation and denial-of-service. In particular, we demonstrate a hill-climbing attack for impersonating a sensor device through variable antenna polarization and show that impersonation is possible when a small number of signals is used for feature extraction. We also show that denial-of-service attacks can prevent accurate identification. Finally, we discuss other attacks and their implications.

4.1 Hill-climbing Attack

A hill-climbing attack is a well known attack on biometric recognition systems [13]. The attack consists of repeatedly submitting data to an algorithm with slight modifications. Only modifications that preserve or improve the matching score are kept in the process. Eventually, a score that exceeds the matching threshold (see Table 2) might be achieved. This results in successful impersonation without providing the genuine biometric.

In order to mount such an attack in our case, we ideally need a specialized device that is able to create similar transient signals (to the ones generated by the sensor nodes) and at the same time allow to introduce variations in it.

We decided to use 3 additional sensor nodes that are not part of the population of 50 sensor nodes used in the evaluation. This provided us with devices able to

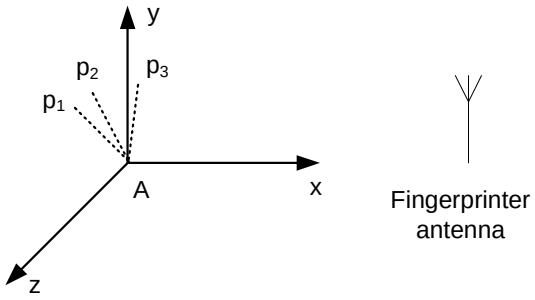

Figure 10: Hill-climbing attack: An intruder sensor device (A) sequentially rotates its external on-board antenna to change the polarization (p_1, p_2, p_3) of the radio waves in order to reduce the similarity score between its own signals and the identification system.

Table 5: Hill-climbing attack summary.

N	50	20	10	5
Hill-attack distance	42.74	38.12	35.89	21.61
Threshold	3.01	4.10	6.74	16.04

generate similar transient signal shapes. In order to create variations in the shapes, we mounted external antennas on these three sensor nodes that are able to change the polarization as shown in Figure 10. This setting was suggested by our analysis of feature stability in Section 3.6.

We collected 50 transient data samples from 7 different polarization positions of the antennas of the 3 sensor nodes. We then supplied these transient data samples to our proposed matching algorithm. Figure 11 displays the similarity scores obtained during the attack in a 3D representation for N=5. For clarity reasons, all scores that exceed the value 100 are not displayed. Table 5 provides the similarity scores obtained against sensor node 9 for N=50,20,10,5.

The identification procedure becomes more vulnerable to hill-climbing with antenna polarization when N decreases. In particular, the matching scores against sensor node 9 for $N = 5$ were consistently very close to the threshold value $T = 16.04$. Device impersonation is therefore highly possible for $N \leq 5$.

4.2 Denial-of-Service Attacks

Due to the low output power and limited spectral diversity of sensor node transceivers, wireless sensor networks are particularly vulnerable to jamming-based denial-of-service attacks [22]. We therefore decided to jam the radio signals of our sensor nodes and quantify the effect of jamming.

We collected transient data samples in presence of a jammer. For jamming purposes we used an USRP device with the GNU radio software [23]. Figure 12 display different transient data samples acquired in presence of a Gaussian noise jamming signal.

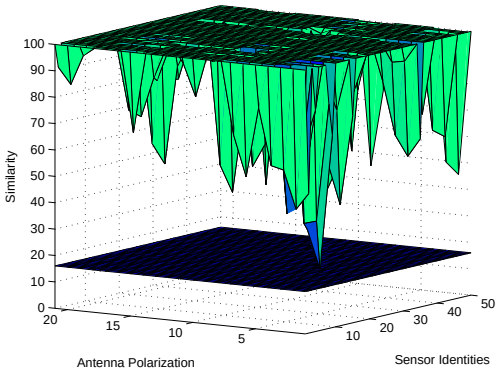

Figure 11: Hill-climbing attack scores: the X-axis contains the 21 (3 sensor nodes x 7 antenna polarization) attacking features; the Y-axis shows the reference features of the 50 sensor nodes targeted for impersonation; the Z-axis is the similarity score obtained between each attacking and reference features. The bottom blue surface is the uniform threshold used for recognition (T=16.04).

Matching experiments showed that it was impossible to successfully recognize the device due to the superposition effect of the jamming and the original sensor node signal. Furthermore, even jamming a small amount of the sensor node signals (5-10 out of 50 that formed the template features) was sufficient to prevent accurate recognition. These findings shows that an identification procedure based on physical signal characteristics must be complemented by a jamming detection mechanism.

It should be noted that a sophisticated jammer can at least theoretically jam only the transient part of the signal, which will result in successful data transmission, but inaccurate identification. So, there is a need for devising a jamming detection procedure not only on the data layer [22, 24], but also for the signal transient.

Other denial-of-service attacks could be potentially devised such as intentionally heating the circuit of the sensor node in order to introduce sufficient variability to prevent accurate identification. However, such attempts might be easily detected by appropriate temperature sensors or tamper-responsive shielding [25].

4.3 Other Attacks

The possibility for recording the transient part of the signal and subsequently concatenating it to a data transmission part for launching a replay attack needs to be investigated. There is a number of points to be considered which makes this attack very hard to achieve. First, the replaying device needs to have a 0 length transient in order to successfully transmit the origi-

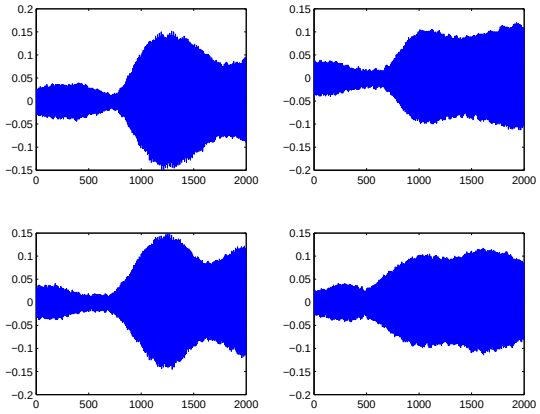

Figure 12: Transient data samples in presence of Gaussian noise jamming.

nal recorded transient. Second, concatenation needs be also very precise to allow accurate demodulation of the signal for data extraction. Third, replayed transient part features will score exactly the same similarity value when matched to the reference template features of the attacked device. This makes the attack easily detectable unless some variability is introduced to prevent same matching score and at the same time the introduced variability needs to stay within the genuine distribution scores of the attacked device. This is not trivial to achieve as demonstrated in our hill-climbing attack.

Hardware circuit replication (cloning) is another attack that can be performed to compromise the system. The instrumentation of such an attack needs physical sensor node capturing and subsequently very accurate replication of the circuitry (i.e., matching as much as possible the characteristics of all integrated circuit components). If, in addition, the devices are equipped with special shielding or a node capture detection mechanism is in place, such a task becomes even harder.

5. APPLICATION SCENARIOS

In this section, we provide more details about possible applications of physical layer identification in all-wireless multi-hop sensor networks.

In a wormhole attack [10], an attacker forwards packets received at one point of the network to another point that is usually multiple hops away. This is achieved by tunneling between two attackers' devices positioned at the respective points. This attack is particularly harmful to routing protocols [26] and very challenging to detect because it can be executed by external attackers and the packet information does not need to be changed. Physical-layer identification will help identifying the attacker's device (intruder) when trying to forward packets, as the physical characteristics of the signal emitted will defer. Such detection can be achieved by a centralized or distributed approach detailed in [9].

Physical-layer identification can be used to prevent Sybil [11] and node replication (cloning) [12] attacks. In the Sybil attack, the attacker gives several identities to the same sensor node with the purpose to fool routing and data aggregation in the network. The replication attack consists of assigning the same (legitimate) identity to several nodes. With a physical-layer identification mechanism in place, and given the difficulty of compromising the identification, these attacks can successfully be prevented.

Physical-layer identification can also be used to complement cryptography-based protocols for authenticating the communication between sensor nodes. It provides a second layer of security that cannot be easily subverted even if the attacker has compromised or was in the possession of the cryptographic keys for communication (internal attacker).

6. BACKGROUND AND RELATED WORK

Radio signal detection/identification gained interest in the early development of radar systems during the World War II [27]. In a number of battlefield scenarios it became critical to distinguish own from enemy radio transmitters on various war-crafts (i.e., planes).

The proliferation of radio technologies in mid and late 90's triggered a number of research initiatives to detect illegally operated radio transmitters [1, 28, 29], device cloning [30] and defective transmission devices (e.g., quality test) [31] by using physical characteristics of the transmitted signals [2].

More recently, physical characteristics of the transmitted signals, in particular the turn-on transient part attracted attention from the wireless community with an attempt to enhance existing intrusion detection schemes usually based on MAC address authentication by a second layer of security based on physical device authentication [32, 17], referred commonly to as radio frequency (RF) fingerprinting. The transient part of the signal includes unique characteristics, that cannot be easily forged unless the circuitry is accurately replicated (e.g., structure, capacitors, resistors, etc.)

These approaches consist of two main parts: 1) Detection and separation of the turn-on transient part of the signal. The accuracy depends on various factors (e.g., channel noise, radio hardware) and has been shown to be critical for such systems [33, 34]. 2) Feature extraction and classification. This part consists of identifying discriminant features in the transient for successful signal classification.

The feature extraction varies from using pure transient characteristics (e.g., amplitude variation, phase) [1, 3, 35, 9, 17] to using frequency characteristics using wavelets [29, 30, 31]. As for classification, a large variety of classifiers has been explored depending on the

application. Genetic algorithms and PNN have been used by [1, 17]. Self-Organizing Maps have been used in [35]. Learning vector quantization (LVQ) was used to distinguish defective from good quality devices [31].

Below, we present the most relevant work to ours in terms of signal similarities, features and purposes.

Hall et al. [3, 32] explored a combination of features such amplitude, phase, in-phase, quadrature, power and DWT coefficients of the transient part. They tested the system on 30 IEEE 802.11b transceivers from 6 different manufacturers and achieved an average classification rate of 94.5%. The error rate highly depended on the device's manufacturer.

Ureten et al. [17] extracted the envelop of the instantaneous amplitude by using the Hilbert transformation and classified the signals using a Probabilistic Neural Network (PNN). They tested their system on 8 IEEE 802.11b transceivers from 8 different manufacturers and registered 96%-98% successful classification.

Both works differ from ours in terms of features used, type and structure of the wireless devices. They used devices from different manufacturers which eases the classification task due to significant differences in the transients signals. An attacker could easily compromise such a system by simply using an identical device.

Rasmussen et al. [9] followed a similar approach to [3, 32] and explored transient length, amplitude variance, number of peaks of the carrier signal, difference between normalized mean and the normalized maximum value of the transient. They tested their system on 10 identical IEEE 802.15.4 wireless sensor devices and achieved a classification accuracy of ∼70%. This work is the closest to ours as it considered wireless sensor devices from the same model and manufacturer, but it differs in the signal capturing process (15 cm from the antenna) and feature extraction. No feature stability, nor attacks were considered.

Very recently, Brik et al. [21] proposed a wireless device identification based on the variance of errors in the modulation domain. They tested their approach on over 100 identical 802.11b NICs, at a distance of 3 to 15 m from the capturing antenna and claimed classification error of 3% and 0.34% for k-NN and SVM classifiers respectively. No evidence about feature stability, nor attacks have been presented.

Our work also differs from the related work in terms of the analysis of identification accuracy. We adopt Equal Error Rate (EER) and Receiver Operating Characteristic (ROC).

Classification vs. Recognition: Classification is a process of classifying test samples to a number of predefined classes of samples. While classification is the right approach for applications with well known type and number of classes (e.g. normal vs defective devices [31]), it is not appropriate for security applications such as intrusion detection, wormhole and Sybil attack detection, etc. The reason is twofold: First, in intrusion related applications, the number of classes (i.e. devices) is unlimited. Second, a standard classifier will classify test signals coming from a device that does not belong to the considered classes of devices to one of the considered classes. Therefore, such applications must be evaluated through their recognition accuracy (EER/ROC) and not classification. Such an evaluation was tried in [32] and very recently in [21]; in fact instead of recognition, these techniques were evaluated using standard classification procedures. It should be noted that standard classification can be adapted for recognition by considering doubt and outlier classes.

Feature stability and attacks: The discussed related works on transient analysis [32, 17, 9] considered only signal acquisition close to the capturing antenna (15-20 cm), which is highly impractical. We believe this is due to the need to compensate the channel attenuation, and unless the appropriate circuit is in place, the identification accuracy drops drastically. None of the works considered the stability of their features with respect to distance, antenna polarization, voltage, nor the attacks on the recognition system.

7. CONCLUSION

In this work, we presented an improved method for capture and analysis of IEEE 802.15.4 sensor node radio signals for enabling reliable and highly accurate identification. Experimental evaluation demonstrated a recognition accuracy with an EER=0.24% which is comparable to state-of-art biometric fingerprint recognition systems. We further analyzed the stability of our method in terms of distance, antenna polarization, voltage and temperature. We showed that our method can successfully identify a sensor node from larger distances as long as antenna polarization does not change over time. We also proposed and performed a number of attacks, namely a hill-climbing attack for device impersonation and denial-of-service jamming attack to test the efficacy of physical-layer identification under various security threats. We believe that this work provides useful insights into the utility (trade-offs and limitations) of physical sensor device identification based on transient analysis for securing wireless sensor networks.

Acknowledgments

The authors would like to thank Kasper Bonne Rasmussen for helping with the initial hardware setup; and Hansruedi Benedicker for his invaluable suggestions in optimizing the signal capturing process, testing the accuracy of individual hardware components and lending quality measurement equipment needed for the experiments performed in this paper. We also acknowledge Thomas Schmid for providing assistance in the project.

The work presented in this paper was supported by the Zurich Information Security Center (ZISC).

8. REFERENCES

[1] J. Toonstra and W. Kisner, "Transient analysis and genetic algorithms for classification," in *Proc. IEEE WESCANEX*, 1995.

[2] K. Ellis and N. Serinken, "Characteristics of radio transmitter fingerprints," *Radio Science*, vol. 36, pp. 585–597, 2001.

[3] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Proc. CIIT 2004*, 2004.

[4] S. Bratus, C. Cornelius, D. Peebles, and D. Kotz, "Active behavioral fingerprinting of wireless devices," in *Proc. ACM WiSec*, 2008.

[5] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Randwyk, and D. Sicker, "Passive data link layer 802.11 wireless device driver fingerprinting," in *Proc. USENIX*, 2006.

[6] T. Kohno, A. Broido, and K. Claffy, "Remote physical device fingerprinting," *IEEE TDSC*, vol. 2, no. 2, 2005.

[7] "Nmap security scanner." http://www.insecure.org/nmap/2004

[8] "Xprobe." http://www.sys-security.com

[9] K. Rassmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Proc. SecureComm*, 2007.

[10] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE INFOCOM*, 2003.

[11] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis and defenses," in *Proc. IEEE IPSN*, 2004.

[12] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE S&P*, 2005.

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

[14] "Fingeprint verification competitions (fvc)." http://bias.csr.unibo.it/fvc2006/

[15] "IEEE 802.15.4 standard," 2006.

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

[17] O.Ureten and N.Serinken, "Wireless security through rf fingerprinting," *Canadian J. Elect. Comput. Eng.*, vol. 32, no. 1, Winter 2007.

[18] B. Moghaddam and A. Pentland, "Probabilistic visual learning for object representation," *IEEE PAMI*, vol. 19, no. 7, pp. 696–710, 1996.

[19] W. Zhao, R. Chellappa, and A. Krishnaswamy, "Discriminant analysis of principal components for face recognition," in *Proc. Conf. on Automatic Face and Gesture Recognition*, 1998, pp. 336–341.

[20] O. Tekbas, N. Serinken, and O. Ureten, "An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions," *Canadian J. Elect. Comput. Eng.*, vol. 29, no. 3, 2004.

[21] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. ACM MobiCom*, 2008.

[22] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM MobiHoc*, 2005.

[23] "Gnu software radio." http://www.gnu.org/software/gnuradio/

[24] M. Strasser, C. Poepper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. IEEE S&P*, 2008.

[25] S. Weingart, "Physical security devices for computer sub- systems: A survey of attacks and defenses," in *Proc. CHES*, 2000.

[26] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proc. IEEE Workshop on Sensor Network Protocols and Applications*, 2003.

[27] R. Jones, *Most Secret War: British Scientific Intelligence 1939-1945*. Hamish Hamilton, 1978.

[28] J. Toonstra and W. Kisner, "A radio transmitter fingerprinting system odo-1," in *Canadian Conf. on Elect. and Comp. Engineering*, 1996.

[29] R. Hippenstiel and Y. Payal, "Wavelet based transmitter identification," in *Proc. ISSPA*, 1996.

[30] D. Kaplan and D. Stanhope, "Waveform collection for use in wireless telephone identification," U.S. Patent 5,999,806, 1999.

[31] B. Wang, S. Omatu, and T. Abe, "Identification of the defective transmission devices using the wavelet transform," *IEEE PAMI*, vol. 27, no. 6, pp. 696–710, 2005.

[32] J. Hall, M. Barbeau, and E. Kranakis, "Radio frequency fingerprinting for intrusion detection in wireless networks," *Submission to IEEE TDSC (Electronic Manuscript)*, 2005.

[33] D. Shaw and W. Kisner, "Multifractal modeling of radio transmitter transients for classification," in *in Communications Power and Computing*, 1997.

[34] O. Ureten and N. Serinken, "Detection of radio transmitter turn-on transients," in *Electronic Letters*, vol. 35, 2007, pp. 1996–1997.

[35] O. Tekbas, O. Ureten, and N. Serinken, "Improvement of transmitter identification system for low snr transients," in *Electronic Letters*, 2004.