Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach

Irwin O. Kennedy,
Patricia Scanlon, Francis J. Mullany

Bell Laboratories
Alcatel-Lucent
Blanchardstown, Dublin 15
Republic of Ireland
irwinkennedy@alcatel-lucent.com

Milind M. Buddhikot

Bell Laboratories
Alcatel-Lucent
Murray Hill, New Jersey
USA

Keith E. Nolan,
Thomas W. Rondeau

CTVR
Trinity College Dublin
Dublin
Republic of Ireland

Abstract

We present a novel technique for radio transmitter identification based on frequency domain characteristics. Our technique detects the unique features imbued in a signal as it passes through a transmit chain. We are the first to propose the use of discriminatory classifiers based on steady state spectral features. In laboratory experiments, we achieve 97% accuracy at 30dB SNR and 66% accuracy at 0dB SNR based on eight identical Universal Software Radio Peripherals (USRP) transmitters. Our technique can be implemented using today's low cost high-volume receivers and requires no manual performance tuning.

1. Introduction

In this paper we describe a new technique for identifying a radio transmitter via RF fingerprinting. Our technique exploits the aggregate effect of differences introduced during transmitter manufacturer. Differences in component design (filters, power amplifiers, inductors, capacitors), same component manufacturing tolerance spread, PCB materials and PCB soldering etc. These differences are imbued in the transmitted signal the and effect can be detected at the receiver. Our method assumes the receiver's frequency response remains constant. The only differences in the digital baseband samples produced by the receiver's radio are due to different transmitters and noise and interference.

Identification of a radio transmitter at the physical layer would enjoy many applications. Gerdes et al.[2] give a diverse list of possibilities; intrusion detection, authentication, forensic data collection and defect detection monitoring. Our work was motivated by a cellular wireless application of femto basestations[5]. This application is a special case of authentication. It involves reducing the core network signalling load due to location management in GSM and UMTS cellular networks. As cells reduce in size, it often desirable to limit cell access to only a subset of an operator's subscriber base. For example, an end customer may install a femto base station and expect exclusive access to it. That is, other mobile phones on the same network may sense the femto cell but when they attempt to camp on it they are to be denied access. From a logical view point denying access is straightforward. The tempory ID provided by the handset is mapped to an absolute ID via signalling to the core network. Based on this absolute ID the femto either permits or denies access. However the large increase in cells and resulting large increase in location area updates means the core network experiences a very large increase in signalling. If we can identify a mobile phone at first contact with the basestation using RF fingerprinting, we can provide an elegant solution to the challenge of supressing signalling traffic at higher layers.

The rest of the paper is organised as follows. We start in Section 2 by reviewing the previous work described in the literature. In Section 3 we describe our proposed approach and in Section 4 we describe our experimental setup and how we capture the data for testing our approach. Finally, we present the results in Section 5 and conclude in Section 6.

2. Background and Previous Work

Several researchers have reported the possibility of identifying a radio transmitter by analysing the received signals. This work stretches back to 1940s and radar transmitter identification [6]. The majority of techniques focus on transmissions at the physical layer.

Physical layer fingerprinting techniques may be split into

two groups: transient signal techniques and steady state signal techniques. A transient signal is transmitted upon transmitter stage power up and power down. It is the short period (typically micro seconds) during which capacitive loads charge or discharge, the power amplifier ramps its power output and in some cases, where the frequency synthesizer makes the transition between steady state frequency generation and being powered off. The steady state period of signal transmission is defined here as the period between the start and end transients.

We are only aware of one example in the literature of studying the steady state signal [2]. The main reason for this is the apparent lack of a steady state signal common to all devices. That is a steady state signal that is either unmodulated or contains the exact same data modulation. This property is important since the signal provides a benchmark for discovering difference between transmitters. By contrast, almost every radio radiates a transient signal upon switch-on and switch-off. For this reason, transient analysis has enjoyed the most attention in the literature [4, 8, 9, 10, 11].

Transient analysis discriminates using the minor amplitude variations that occur upon transmitter switch on. Due to the short duration of transient signals, very accurate and consistent detection of the transient part of the signal is important for good identification performance. However, it also poses the most significant challenge. The receiver architecture is unusual since it must be capable of digitising at extremely high sample rates. This is necessary to provide the granularity of amplitude information required for the transient feature extraction algorithms. For example 5 GSamples/s is used by Serinken et al. [1, 9] and 500 MSample/s is used by Hall et al. [3]. The two key approaches are the threshold [8] and Bayesian step change detector [10, 11]. Both rely on reception at high SNR and an abrupt change at the start of the transient - both of which may not exist in practice. A third approach based on frequency domain analysis was recently proposed by Hall et al. [4]. Rather than relying on amplitude characteristics for start and end time estimation, the authors were able to produce reasonable estimates by analysing the variance of its spectral components under high SNR conditions. However, as noted by the authors, it is not yet known to what extent it is possible to find distinguishing characteristics in the transients in larger device sets. Others have reported that the level of difference between identical transmitters manufactured by the same company may not be distinguishable using transient analysis [1]. Where it is possible to reliably detect the transient start and end points, several researchers have reported good classification performance. In excess of 90% for high SNR environments [3, 8, 9].

The lack of a steady state signal common to all transmitters is no longer the case in modern transmitters. Today's digital transmitters intentionally introduce repetitive sequences such as preambles to simplify receiver design. This makes steady state signal analysis feasible today. Recently Gerdes et al. [2] proposed that analysing the steady state signal may provide the ability to distinguish between same model cards manufactured by the same company. They argue that the transient signal is so short that it cannot contain enough information to discriminate between similar devices. Their focus is on wireline transmitters where similar principles apply. A portion of the IEEE Ethernet 802.3 frame preamble common to all devices was identified and used to construct a device fingerprint. They use a matched filter implementation and simple thresholding to perform classification. Training involves characterising the matched filter's output to determine the output magnitude that corresponds to a match for a particular transmitter. The discriminatory capabilities of this approach are unclear. No overall level of acuracy is provided. It appears that the thresholding decision for device identification can result in more than one device being identified. The result is many false-positive identifications. Their system also requires many ad hoc steps to tune the performance. For example, the discriminatory performance was manually refined through a combination of bandpass filtering, creating an ensemble of matched filters and time domain trimming.

In summary, physical layer fingerprinting offers promise for passive discrimination between a large set of wireless transmitters. We note that:

1. Transient analysis offers good classification performance only where the begining and end of the transient can be reliably identified.

2. It has been reported in [1, 2], that transient analysis is not always able to distinguish between same manufacturer/same model variants.

3. The very high sample rates demanded by transient analysis requires sophisticated and expensive receiver architectures.

Steady state signals offer a relatively unexplored alternative to transient analysis. We note that if discrimination is possible in the frequency domain, the use of standard low cost ADC sample rates and receiver architectures will be made possible.

3. Method

Our approach to RF fingerprinting uses frequency domain analysis combined with traditional discriminatory classifiers to perform device identification. When compared to the only known previously published steady state technique[2], our technique offers a significant performance improvement through more flexible feature selection and

the use of a k-NN discriminatory classifier. Our work is distinguished from the large body of previous work on transient based analysis by its focus on the steady state portion of the signal. The main advantage over transient analysis is that it can be implemented using todays low-cost radio receiver front ends e.g. ethernet access points or femto cells. These radio receivers capture the signal at sufficiently high sample rates for our proposed approach. By contrast, transient based approaches require very high sample rates to capture the amplitude fluctuations of the transient part of the signal.

Figure 1 illustrates the processing steps involved in device identification. The input to the preprocessing stage is the received RF signal from the transmitter. For convenience we constrain the higher layers of the communications system to transmit exactly the same signal every time. Handing more than one signal is just a matter of implementation. For example, for the RACH preamble in UMTS, the signature and uplink scrambling code pair are constrained to a single combination, rather than the usual 16-48 different combinations. A standard radio receiver architecture is employed, downconverting the transmit band to baseband, before being bandpass sampled by the ADC at the Nyquist rate.

The next step in Figure 1 is carrier frequency offset correction. Captured preambles are separated in time by a period of no transmission. The preamble sequences were extracted from the signal prior to downsampling using a sum of the absolute values window function. The window has length equal to the number of samples in a preamble. It is shifted across the file in 10 sample increments, with the total energy recorded for each window. For every set of samples between two periods of no transmission, the window with the maximum energy is extracted as the preamble. No attempt is made to distinguish between transient and steady state portions of the signal. We estimate the complete preamble is extracted with better than 99.99% accuracy relative to its total energy content.

Spectral analysis is then performed on the entire transmitted premable signal. The Fast Fourier transform (FFT) is used to compute spectral components from the time domain steady state portion of the signal and a set of log-spectral-energy features is input to the classifier. Prior to the spectral analysis and to remove amplitude variations that may occur each time the signal is transmitted, the time domain samples are amplitude normalised.

The output of the spectral analysis stage feeds into the final device identification stage in Figure 1. The data collected from each board is divided into two sets. The first set is used in the classification training step and the second test set is omitted from training and used to test performance of the system. The k-Nearest Neighbour (NN) classification technique is employed in the experiments. In the k-NN algorithm the training preambles is mapped into multidimensional feature space which is partitioned into regions based on the class labels. The preamble is said to belong to a particular class if it is the most frequent class label among the k nearest training preambles, where distance is determined using the Euclidean distance metric. In these experiments $k = 5$ is used. In this RF Fingerprinting system each class represents one of the 8 possible Universal Software Radio Peripheral (USRP) transmitter boards. The system is presented with a previously unseen preamble and attempts to discriminate between each of the 8 candidate classes to determine from which board this preamble is obtained from. Classification accuracy is given as the percentage of correctly identified boards.

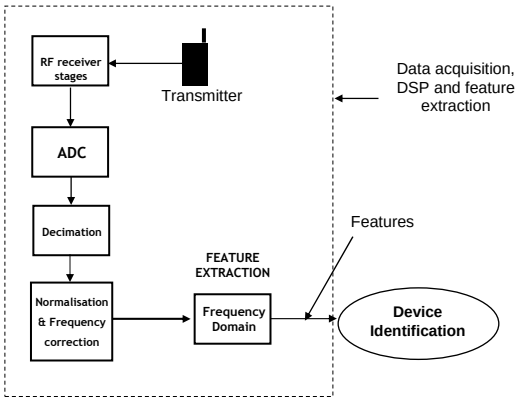

Figure 1. Processing Chain

4. Experimental Apparatus

The test equipment used for the experimental work comprises an Anritsu MG3700A vector signal generator, an Anritsu Signature MS2781A spectrum analyser, and eight USRPs. The USRP is an inexpensive, flexible, and powerful radio front-end for software defined radio operations and experimentation. The USRP consists of a motherboard that houses a FPGA, two DAC/ADC chipsets, four daughterboards, and a USB bus to transfer data and control information. To minimise the potential for interference, each transmission source is connected via a coaxial cable to the spectrum analyser. The Anritsu MS2781A captures received samples of 200 ms in duration from each of the transmission sources.

As observed above, the important property of the preamble is that it is always identical and is repeated often. The details of the preamble are not particularly important, but we based our preamble on the UMTS random access channel (RACH) preamble. To match the nominal bandwidth of the USRP, our preamble occupies a bandwidth of 1MHz and consists of 4096 chips at a rate of 0.768Mcps. The 4096

chip pseudorandom quadrature phase shift keying (QPSK) signal is generated using Matlab. This baseband signal is then passed through a root raised cosine filter of order 40 and excess bandwidth $BT = 0.22$. The transmissions are centered in 2.4 GHz - 2.5 GHz band and each RACH preamble burst is separated by a 0.5 ms null guard interval.

This QPSK-level description of the preamble is transmitted by each of the USRPs. The Centre of Telecommunications Valuechain Research (CTVR) reconfigurable software radio platform, Implementing Radio in Software (IRIS)[7], is used to drive the USRPs. Each USRP is driven identically, so the only difference in the complete transmit chain is simply the transmitter (the circuitry from the DAC through to the antenna).

The receiver used is an Anritsu MS2781A Signature spectrum analyser. It is connected to one RF transission source at a time using a coaxial cable. The analysers output is the baseband digital I/Q samples. The analyser sampled at 50 MS/s which is then decimated to 2 MS/s in software.

We capture a total of 2400 preambles - 300 for each of the eight USRP boards. 150 preambles are used for training purposes and the remaining 150 preambles are used to test the system.

5. Results

We conducted two experiments to measure and help understand the performance of our approach. We collected measurements for eight different USRP transmitters. These transmitter boards have identical specifications, although boards two and six are slightly revised designs (marked Rev 3.0) with a couple of minor component supplier changes. The signals were collected with good SNR via cabelled connections. The MATLAB additive white Gaussian noise (AWGN) function was used to add white Gaussian noise to the signals. The classification performance is graphed in Figure 2. The plot is the achieved classification performance expressed as a percentage against SNR. Based on passing a single RACH preamble into the classifier, 97% classification accuracy above 25 dB SNR was achieved. The performance drops off as expected for lower SNR values, however it still managed to produce results with 66% accuracy for 0 dB SNR.

The second experiment explored the effect of the binning on classification accuracy. The binning functions purpose is to reduce the number of spectral features fed into the classifier. If the number of bins is set to one, a single feature - the mean energy of the complete spectrogram, forms the classifier input. As we increase the number of bins, the frequency granularity is increased. Figure 3 shows the results of this experiment, plotting percentage classified correctly versus the number of bins. The plot is split into two pieces so that we can present the first 200 bins in more detail. We recorded

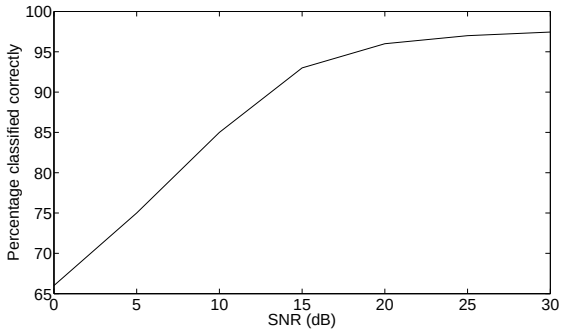

Figure 2. Best recorded classification performance against SNR.

performance every 5 bins under 200 and then every 50 bins between 200 and 2000. As can be seen from the graph, the first 10 bins showed the steepest increase in performance, before the plots levels off. We notice that the lower SNR conditions demand more bins to achieve the maximum classification performance.

We believe that at high SNR, even the smallest spectral energy differences can contribute to discrimination. As the SNR increases the small spectral energy differences start to be destroyed. By increasing the number of bins, we increase the number of spectral energy features. In doing so, we reduce the chance that all features have had their complete discriminatory value destroyed by noise. We note that noise will reduce the discriminatory value offered by the smaller bins, hence even after dividing the energy across many bins, lower overall classification performance is still to be expected at low SNR.

The 15dB-30dB SNR plots have all reached their maximum classification performance by about 200 bins. The 0dB-10dB plots are very close to reaching their maximum classification performance by 2000 bins.

6. Conclusions

We have presented a novel, low-cost approach to transmitter identification using RF Fingerprinting. Our approach performs very well - being able to distinguish between eight identical transmitters with 97% accuracy at 30dB SNR. Performance is still good at 0dB SNR, reporting an accuracy of 66% dB. Our use of the k-NN discriminatory classifier automates creation of the classification engine and the use of the DFT introduces great flexibility into spectral feature selection. Our system is capable of working with common low-cost receiver architectures with no hardware modifications. It therefore offers a lower cost solution to previously proposed transient based approaches which require very high speed ADCs.

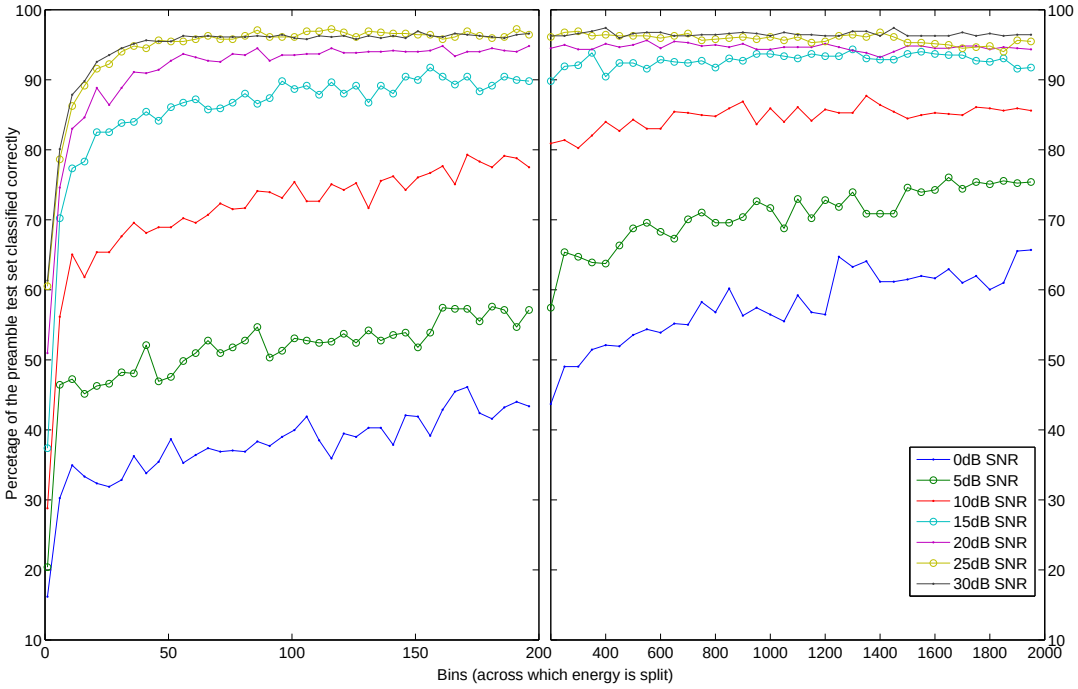

Figure 3. Percentage classified correctly against number of bins for several SNR environments.

In future work we plan to investigate other radio transmitters, techniques to improve performance in high SNR environments and other non-ideal environments. We have reason to be confident that our system will perform well in indoor multipath radio environments due to the typically small delay spread relative to chip rates.

References

[1] K. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints. *Journal of Radio Science*, pages 585–597, 2001.

[2] R. Gerdes, T. Daniels, M. Mina, and S. Russell. Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach. *ISOC Network and Distributed System Security Symposium*, 2006.

[3] J. Hall, J. Barbeau, and E. Kranakis. Detection of Transient in Radio Frequency Fingerprinting using Signal Phase. *Proceedings Wireless and Optical Communications*, 2003.

[4] J. Hall, M. Barbeau, and E. Kranakis. Detecting rogue devices in Bluetooth networks using Radio Frequency Fingerprinting. *Proceedings of the International Conference on Communications and Computer Networks*, 2006.

[5] L. Ho and H. Claussen. Effects of User-Deployed, Co-Channel Femtocells on the Call Drop Probability in a Residential Scenario. *IEEE International Symposium on Personal, Indoor and Mobile Communications*, 2007.

[6] R. Jones. *Most Secret War*. Hamilton, 1978.

[7] P. Mackenzie, L. Doyle, K. Nolan, and D. Flood. IRIS A system for Developing Reconfigurable Radios. *IEE Colloquim on DSP-enabled Radio*, September 2003.

[8] D. Shaw and W. Kinsner. Multifractal Modelling of Radio Transmitter Transients for Classification. *Proceedings Conference on Communications, Power and Computing*, pages 306–312, 1997.

[9] O. Tekbas, N. Serinken, and O. Ureten. An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions. *Canadian Journal Computer Engineering*, 2004.

[10] O. Ureten and N. Serinken. Bayesian detection of transmitter turn-on transients. *Proceedings NSIP99*, pages 830–834, 1999.

[11] O. Ureten and N. Serinken. Detections of radio transmitter turn-on transients. *Electronic Letters*, pages 1996–1997, 1999.