Identification of Legacy Radios in a Cognitive Radio Network Using a Radio Frequency Fingerprinting Based Method

Nansai Hu
Outline

• Cognitive radio overview
• Security, vulnerability challenge
• Radio frequency fingerprinting (RFF)
  – RFF modeling (feature extraction)
  – Machine learning based analyzer
• Summary
Cognitive Radio Overview
Cognitive Radio

- Cognitive radio (CR) / Dynamic spectrum access (DSA)

- Cognitive radio (CR) technology is considered to be a promising technique to improve spectrum utilization by seeking and opportunistically utilizing resources in time, frequency, and space domains without causing harmful interference to legacy systems.

- Cognitive users (unlicensed, secondary users) first sense radio spectrum, detect licensed users (primary users) and then take use of the spectral holes left by the primary users to achieve opportunistic access.
Challenge

- CR’s flexible access method leads to uncertainties to a CR network. There are complex SU misuse issues during its secondary access process, including misbehavior, attack, and cheating (e.g., PUE Attackers).

- Radio identification/classification is an important research issue.

- In literatures, several approaches for radio identification/classification are proposed, including:
  - Modulation recognition;
  - Terminal localization;
  - Transmission protocols classification;

- However, some of these methods are subject to PU emulation or impersonation attacks.
Radio Frequency Fingerprinting Identifications

- **Models:** Radio frequency fingerprinting modeling + RFF analyzer
- **Objective:** Distinguishing radio/user class (legacy radios/users versus secondary radios/users) and individual radio/user terminals (within one class/type)

**Advantage vs. Traditional Approaches**
- Some of the traditional methods are subject to PU emulation or impersonation attacks.
- Radio frequency fingerprinting (RFF) features which are due to hardware imperfection and thus, more difficult to reproduce.

It is not feasible to train all devices before testing in practice. In our work, we extract features of a class of devices and then use this profile to identify the same type of devices.
Radio Frequency Fingerprinting - An RF Transient

Implications of RFF feature and CR’s circuit components

- **Crystal oscillator:**
  - Phase noise
  - RF frequency value;

- **Amplifier:**
  - Rising time;
  - Rising envelope shape;
  - Overshoot and undershoot;
  - DC offset

- **Filter:**
  - Spectrum characteristics of harmonic
RFF modeling
(feature extraction)

• Preprocess the received signal transient through dividing it into two parts: a non-steady part and a steady part;

• In the non-steady part, we extract time related features, e.g., rising time ($T_r$, in number of sampling points) and rising shape ($R_s$, a 10-point amplitude vector for describing the rising edge).

• For the steady part, the spectrum features are extracted through a fast fourier transform (FFT), that is, the frequency value and corresponding amplitude of the second harmonic ($H_a$ and $H_f$) is extracted, as well as the third harmonic ($H_a$ and $H_f$).

• Further, the signal statistical features are also extracted by calculating the positive variance ($PV$), negative variance ($NV$), and the mean value ($MV$) in the steady part of the signal transient.

• We thus have a feature set $X = \langle T_r, H_a', H_f', H_a'', H_f'', PV, NV, MV, R_s \rangle$ \hspace{1cm} (1)
Identification Methodology

• Based on the extracted RFF features, we apply two machine learning (ML) algorithms as the analyzers/classifiers.
  – *Artificial Neural Network*
  – *Support Vector Machine*

• Machine learning algorithms determine the most suitable hypothesis by the current observed data and prior knowledge.
Artificial Neural Network (ANN)

The input to the $j$th hidden unit, $net_p(j)$, is expressed as

$$net_p(j) = \sum_{k=1}^{N} W_{hi}(j,k)X_p(k), \quad 1 \leq j \leq N$$  \hspace{1cm} (2)

With the output activation for the $p$th training instance, $O_p(j)$, is expressed by

$$O_p(j) = f(net_p(j))$$  \hspace{1cm} (3)

The nonlinear activation is typically chosen as a sigmoid function [11]

$$f(net_p(j)) = \frac{1}{1 + e^{-net_p(j)}}$$  \hspace{1cm} (4)

Then, the final output for the $p$th training instance in the output layer is expressed by

$$Y_p(i) = \sum_{k=1}^{N} W_{oi}(j,k)X_p(k) + \sum_{j=1}^{N} W_{oh}(i,j)O_p(j)$$  \hspace{1cm} (5)

Artificial neural network (ANN) is an information processing paradigm which is inspired by biological nervous systems.

- It is composed of a large number of highly interconnected processing elements (neurones) working in unison to solve specific problems [10].
- In this paper, we apply a commonly used neural network model, multi-layer perception (MLP), to solve the radio/user identification problem.
Support Vector Machine (SVM)

- Support vector machine (SVM) is another set of machine learning methods which can be used for classification and regression task.

- More formally, a SVM constructs a complex hyper-plane in a higher order dimensional space (so that the instance of the separate categories are divided by a clear and as wide as possible gap), which can be used to satisfy classification demand easily.
SVM Algorithm

In Eq. (7), the training vectors $X_p$ are mapped into a higher dimensional space by a function $\phi$. SVM finds a linear separating hyperplane with the maximal margin in this higher dimensional space. In Eq. (6), $C > 0$ is the penalty parameter of the error term. Furthermore, $K(X_i, X_j) \equiv \phi(X_i)^T \phi(X_j)$, $(i, j \in 1, 2, ..., p)$ is called the kernel function.

For linear kernel function:

$$K(X_i, X_j) = X_i^T X_j$$  \hspace{1cm} (9)

For radial basis function:

$$K(X_i, X_j) = \exp(-\gamma \| X_i - X_j \|^2), \quad \gamma > 0$$  \hspace{1cm} (10)
To capture an RF transient waveform:
The oscilloscope is configured with a 2GHz sample rate, 500us capture period. Based on the integrated MATLAB software in oscilloscope, the RFF feature extraction time is approximately 0.74s, the identification processing time for SVM algorithm with radial basis function kernel, SVM algorithm with linear function kernel and MLP neural network algorithm are approximately 0.27s, 0.19s, 0.33s, respectively.
Experiment I: Radio/User Class Classification (Legacy Radio vs. Cognitive Radio)

- We configure two USRP terminals to impersonate the MOTOROLA walkie talkie (i.e., program USPR to transmit the same signal as MOTOROLA walkie talkie).
- We implement two machine learning algorithms (SVM with radial basis function and MLP neural network) as the classifiers.
- After a 40-cycle training and a 1000-cycle testing.
Results of radio/User Class Classification

- Rising edge features only, rising time ($Tr$) and rising shape ($Rs$).
- Statistical features only ($PV$, $NV$ and $MV$ in Eq. (1)).
- Frequency response features only ($Ha$, $Hf$, $Ha$, $Hf$ in Eq. (1)).
- All the features in Eq. (1) together
Radio Terminals Identification

• **Experiment II: Radio Terminals Identification within One Radio Type**
  
  – We implement three machine learning algorithms (SVM with radial basis function, SVM with linear kernel function, and MLP neural network).
  
  – After a 20-cycle training and a 500-cycle testing under different SNR levels.
Results of Radio Terminals Identification

- The SVM algorithm with radial basis function performs slightly better than linear kernel function SVM algorithms.

- For the performance of MLP neural network algorithm, it is not as good as SVM algorithm under low SNR conditions and close to SVM method when SNR is high.

- When SNR=10dB, the proposed RFF based method has an approximately 95% correct identification probability on USRP terminals and an approximately 70% correct identification probability on MOTOROLA walkie talkies.
Summary

- In this work,
  - Propose an user/terminal identification method based on radio frequency fingerprinting feature
  - Introduce a multi-dimension RFF feature extraction method considering a signal transient
  - Implement RFF feature extraction and machine learning algorithms in a hardware platform
  - Our future work in this area will include a variable temperature experiments and enhancement in a variety of radio classes/terminals (i.e., apply to more radio types and examine more terminals within one type).
• Thank you.