Detection and Recognition of RF Devices Using Support Vector Machine

Shikhar P. Acharya, Missouri University of Science and Technology, Rolla, MO, USA
Ivan G. Guardiola, Missouri University of Science and Technology, Rolla, MO, USA

ABSTRACT

Radio Frequency (RF) devices produce some amount of Unintended Electromagnetic Emissions (UEEs). UEEs are generally unique to a device and can be used as a signature for the purpose of detection and identification. The problem with UEEs is that they are very low in power and are often buried deep inside the noise band. The research herein provides the application of Support Vector Machine (SVM) for detection and identification of RF devices using their UEEs. Experimental Results shows that SVM can detect RF devices within the noise band, and can also identify RF devices using their UEEs.

Detection and Recognition of RF Devices Using Support Vector Machine (SVM), Unintended Electromagnetic Emissions (UEEs)

INTRODUCTION

Electronic devices with any kind of communication capabilities or which work at RF frequencies emit some amount of Unintended Electromagnetic Emissions (UEEs) (Weng et al., 2006). These emissions are generated by the signals created by a local oscillator for an integrated circuit. Local oscillators emit electromagnetic signals at a fundamental frequency with narrow, continuous wave tones at associated harmonics. These signals then couple with device’s antenna, connection wires, or housing of the device and are radiated outside the device as UEEs (Bole et al., 2009; Sekiguchi & Seto, 2008). An example of UEE is shown in Figure 1.

The characteristics of the UEEs depend upon the characteristics of the receiver, the internal electronics, and the electronic signals within the device (Weng et al., 2005). There always exist some differences between various internal electronic components like registers and transistors between different devices. For example, no two resistors are exactly the same as all manufactured resistors are created within a tolerance. Hence, the combination of the characteristics of these components are unique to each device, UEEs generated by these devices will also be unique. The uniqueness of these features of the UEE signals from a device can therefore reveal information about an electronic device’s internal state (Sekiguchi & Seto, 2008). UEEs can thus be taken as a unique signature of

DOI: 10.4018/ijitn.2013100102
electronic devices that can be used for device detection and identification.

Detection of RF devices through UEEs has many applications. A recent example is the interference of wireless devices in airplane communications. It was taught that interference from mobile devices might pose a significant threat to aircraft communication and radio navigation receivers (Ely et al., 2002). Therefore, airplane passengers are required to power off their electronic devices during take-off and landing. However, recently the FAA has relaxed these restrictions. There are other places like customs office and courthouses where the use of wireless devices is sometimes prohibited. These devices may be used to illegally record or interrupt the proceedings (Tryon, 2008). Another undesirable use of wireless devices is to remotely detonate Improvised Explosive Devices (IEDs). There are two methods to detonate an IED. First method is to wire the explosive material to the RF receiver directly. A call is then made to that phone which acts as the detonator. Another method is to set a timer using the internal alarm of the RF receiver. The IED will detonate when the alarm is triggered (Strother, 2007).

One way of controlling undesired and illegal usage of wireless electronic devices is to detect them while in use. The identification and detection of wireless devices in prohibited areas will help to minimize the harmful effects of such usage. Flight attendants, for example will be able to make sure if all the devices are turned prior to take off and landing. Security officers like bailiff of courts can determine if there is an illegal usage of devices in prohibited areas. Army personnel can identify and locate IEDs in potential area and safely deactivate it. However, there are also commercial uses for the detection of wireless devices. One example, is tracking customers in a retail store. Or detection of vehicles to manage and control traffic in congested urban roads.

In this paper we exploit the use of the Support Vector Machine as a means to first recognize wireless communication devices solely through their UEEs. In addition, this paper seeks to demonstrate that through relatively simple analysis the recognition and identification of wireless devises can be accomplished through these low power signals. Lastly, this demonstrates the passive detection capability without the need to stimulate the wireless device in question. The remainder of this paper is organized by first demonstrating the literature associated with this problem, which motivates the need for an efficient method recognition.
Power and Latency Optimized Deadlock-Free Routing Algorithm on Irregular 2D Mesh NoC using LBDRe
www.igi-global.com/article/power-and-latency-optimized-deadlock-free-routing-algorithm-on-irregular-2d-mesh-noc-using-lbdre/89260?camid=4v1a

Modeling and Simulation of Traffic with Integrated Services at Media Getaway Nodes in Next Generation Networks
www.igi-global.com/chapter/modeling-simulation-traffic-integrated-services/72424?camid=4v1a