Chapter 15
Security of Wireless Devices using Biological-Inspired RF Fingerprinting Technique

Saeed ur Rehman
Unitec Institute of Technology, New Zealand

Shafiq Alam
University of Auckland, New Zealand

Iman T. Ardekani
Unitec Institute of Technology, New Zealand

ABSTRACT

Radio Frequency (RF) fingerprinting is a security mechanism inspired by biological fingerprint identification systems. RF fingerprinting is proposed as a means of providing an additional layer of security for wireless devices. RF fingerprinting classification is performed by selecting an "unknown" signal from the pool, generating its RF fingerprint, and using a classifier to correlate the received RF fingerprint with each profile RF fingerprint stored in the database. Unlike a human biological fingerprint, RF fingerprint of a wireless device changes with the received Signal to Noise Ratio (SNR) and varies due to mobility of the transmitter/receiver and environment. The variations in the features of RF fingerprints affect the classification results of the RF fingerprinting. This chapter evaluates the performance of the KNN and neural network classification for varying SNR. Performance analysis is performed for three scenarios that correspond to the situation, when either transmitter or receiver is mobile, and SNR changes from low to high or vice versa.

INTRODUCTION

The inventor of wireless communication, Guglielmo Marconi demonstrated the communication of telegraphic messages in the late nineteen-century. Since then, the world has seen an explosive growth in the field of wireless communication. Particularly in the last ten years, several new wireless technologies have been invented to expand the growing application of wireless communications. In the coming days, wireless modules will be embedded in various objects, such as home

DOI: 10.4018/978-1-4666-6078-6.ch015

appliances, transport, clothes, gadgets, toys, food carts, roads, bridge, farms, buildings, animals and people.

The continued proliferation of inexpensive wireless Radio Frequency (RF) devices provides worldwide communication connectivity to virtually every individual. These wireless devices broadcast information to intended recipients in the form of an electromagnetic emission. However, the electromagnetic emission may be remotely monitored, recorded, intercepted or analyzed by unintended recipients owing to the broadcasting nature of the wireless medium. Generally, the communicators are unaware of this activity, and moreover, the intentions of unintended recipients vary. The unintended recipient may simply listen to the communication activity and remain passive – an activity that is difficult to detect– or may become active and compromise the identity of the wireless device by launching "spoofing" or "man in the middle" type attacks (Meyer & Wetzel, 2004). For example, the software within a wireless device allows the Medium Access Control (MAC) address of a network interface card to be modified and thus it is vulnerable to a spoofing attack (Faria & Cheriton, 2006). Similarly, the Erasable Programmable Read Only Memory (EPROM) of a cellular phone carries the phone's Electronic Serial Number (ESN) and Mobile Identification Number (MIN), which can be changed by replacing the EPROM, hence allowing the identity of the phone to be changed (Nguyen, et al., 2011). Compromising the identity of wireless devices makes them vulnerable to a variety of attacks, which can take the form of impersonation, intrusion, theft of bandwidth and denial of service.

To increase network security and mitigate identity theft attacks, much of the research is focused on traditional bit-level algorithmic. In conventional wireless networks, security issues are primarily considered above the physical layer and are usually based on cryptographic methods, where the cryptographic algorithms are mainly used for establishing the identity of a legitimate wireless device. A two-way communication is required to establish a session key in the cryptography. However, the security algorithm would be compromised upon access to the key, thus making it difficult to distinguish a legitimate key/device and cloned key/device (Mathur, et al., 2010). Additionally, higher-layer security key distribution and management may be difficult to implement and may be vulnerable to attacks in some environments, such as ad-hoc or relay networks, in which transceivers may join or leave randomly (Debbah, 2008; Kauffmann, et al., 2007). Furthermore, some recent wireless technologies do not allow an interactive communication for establishing a cryptography key due to its unique architecture. One such example is Cognitive Radio Network (CRN), which is invented in order to increase the efficient utilization of the spectrum. However, if a Primary User Emulation (PUE) attack is launched then the whole operation of CRN is jeopardize by effectively limiting the access of legitimate users to idle spectrum (Chen, et al., 2008).

More recently consideration has been given to detecting and mitigating spoofing near or at the bottom of the Open Systems Interconnection (OSI) network stack. One such work includes the addition of a "lightweight security layer" hosted within the Medium Access Control (MAC) layer to detect spoofing and anomalous traffic (Li & Trappe, 2007). Other recent efforts have focused on Physical (PHY) layer implementations with a goal of exploiting RF characteristics (radio and environmental) that are difficult to mimic, thus minimizing the opportunity for spoofing. Hence, identity theft can be effectively tackled using physical layer security. Physical layer security based on the extraction of unique feature from the analog signal is called RF fingerprinting.

The classification process of RF fingerprinting can be divided into training phase (for generating the profile RF fingerprint of a specific transmitter) and the testing phase (for identifying the wireless device). Majority of the existing RF fingerprinting techniques have either used high SNR signals or