Cognitive Radio Networks and Security Threats

The allocation of the Industrial, Medical and Scientific (ISM) band has enabled the explosion of new technologies (e.g. WiFi) due to its licence-exempt characteristic. Millions of users worldwide can enjoy anywhere-anytime and affordable Internet access, with devices (e.g. laptops, smartphones, etc.) that operate in the ISM band.

Nowadays, the explosion of plethora of applications based mainly on the social media, and the Internet-of-Things (IoT) paradigm, usually causes overcrowding in this band, with undesired consequences. Overcrowding in the free spectrum often creates harmful interference, and wireless channel contention between the networking devices that cause link quality degradation, and poor network performance, negatively affecting user experience.

On the other hand, several studies (e.g. [1, 2]) have shown that licensed band utilisation is low, and according to FCC [3], temporal and geographical variations in the assigned spectrum can range from 15% to 85%. These free (un-utilised or under-utilised) portions of the spectrum are called as *spectrum holes* or *white spaces*.

Cognitive radio (CR) technology has emerged as a solution to the spectrum under-utilisation issue. CR-enabled devices can sense (detect) the spectrum holes, and use them in an opportunistic manner. In general, spectrum users are divided into two categories: (i) primary or incumbent users (PUs) that hold a license for a specific portion of the spectrum, and (ii) cognitive or secondary users (SUs) that use parts of the spectrum in an opportunistic way. SUs can make use of the CR technology and transmit in the licensed vacant bands. However, CR technology should cause minimum interference to PUs, and when a PU signal is detected, SUs shall immediately stop transmitting in this band.

CR technology, as every wireless network technology, faces a number of security threats and attacks, due to the open medium used for the transmissions. Common attacks for these technologies include MAC spoofing, jamming and congestion attacks, small back-off window attacks, etc.

Additionally to these attacks, CR networks face new types of attacks because of their two unique features: (i) *cognitive capability* that enables the CR devices to sense the environment and select the best available spectrum portions, and (ii) *re-configurability* that makes feasible for the CR devices to change on-the-fly several of their transmission characteristics (e.g. frequency, modulation, transmission power, etc.).

Attackers by taking advantage of the cognitive capability of CR devices, can mimic incumbent transmitters so as to enforce SUs vacate the specific band. This attack is referred as *primary user emulation attack* (PUEA), and can be regarded as a DoS type of attack. PUEAs can also be launched by greedy users aiming to force all other users to vacate a specific band, and acquire its exclusive use.

For the detection of PUEAs, many state-of-the-art contributions assume that the locations of the PUs are known in advance (e.g. [4, 5]). During operation, and when an incumbent signal is detected, several algorithms considering physical layer characteristics, for example the Received-Signal-Strength-Indicator, can estimate the location of the transmitter, and then compare it to the known PU locations, and infer about if a PUEA is in progress. Other works assume that no a-priori knowledge of the PUs is available, and try to detect fake primary signals using characteristics of the multi-path components, like the ratio of the first and the second multi-path components of the received signal at a helper node that is located very close to a PU.

Another type of attack against CR networks is the *spectrum sensing data falsification* attack (SSDF). Assume a CR network where SUs take part in a distributed spectrum sensing scheme, reporting their findings to a fusion centre (FC) that decides about spectrum availability, based on the observations from all SUs. Such distributed schemes aim to address issues related to undetected primary signals due to signal fading, multi-path, etc. A user can take advantage of this scheme, by reporting false observations to the FC; this is the SSDF attack.

The motives for this attack can vary, and a malicious user aims to make FC or other SUs to falsely conclude that PUs are active, or make them believe there are no active PUs when there are. In the last case, harmful interference will be created for the PUs. In other situations, greedy users launch SSDF attacks with the goal to monopolise a specific band by forcing all other SUs to evacuate it. In all cases, the reliability of the distributed scheme is severely degraded by the faulty observations.

For the detection of these attacks, the proposed algorithms (e.g. [6, 7]) adopt trust-based schemes where several fusion rules are used by the FC (AND, OR, average, Dempster-Shafer theory of evidence, etc.). Based on these schemes, the reputation of each SU is estimated, and if an SU is characterised as an adversary, its reports are ignored by the FC.

Both PUEA and SSDF, are severe attacks that can be easily implemented with off-the-shelf hardware and affect all parts of the so-called *cognitive cycle* (Figure) [8].

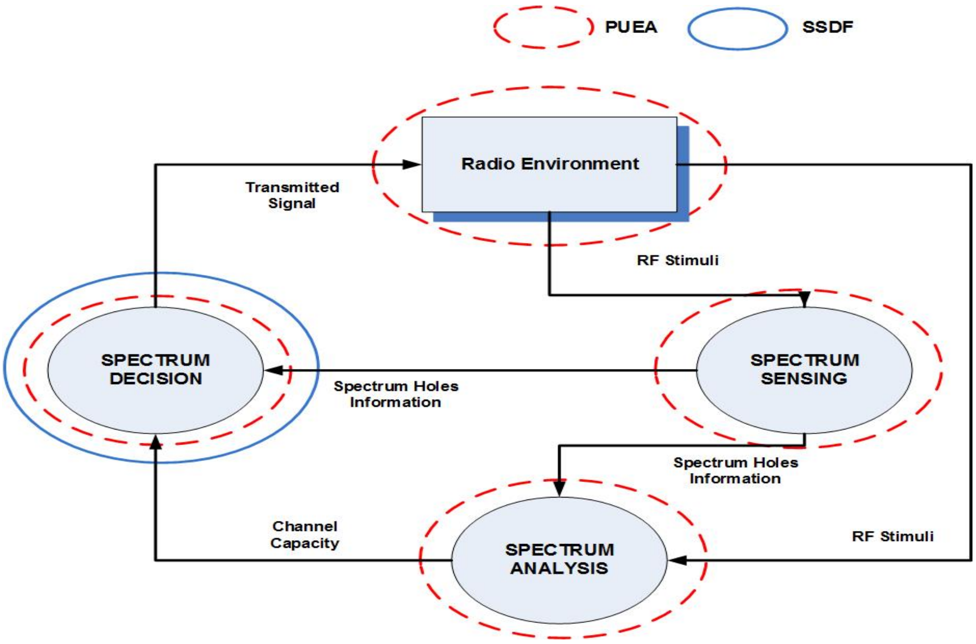

Figure The cognitive cycle

CR research focusing on several areas (security, spectrum sensing, spectrum analysis, etc.) has been significantly boosted using Software-Defined Radios (SDRs), devices that are highly re-programmable. SDRs allow for on-the-fly re-configuration of several parameters like the frequency, modulation, transmission power, etc.

In our laboratory, the Telecommunications and Networks Lab of ICS-FORTH (https://www.ics.forth.gr/tnl/index_main.php?l=e&c=275), we follow a vertical approach to the SDR technology, providing everything, from higher layer software functionality and optimization, down to driver and hardware design of devices. Accordingly, we have developed an SDR based platform that is able to efficiently support heterogeneous wireless standards. Our platform enables the concurrent transmission and reception of multiple standards and channels, within the same radio band, utilizing a single workstation with open-source software and an SDR device. Two prevalent standards of IoT, the IEEE 802.11 & 802.15.4, are fully implemented in software, and are able to simultaneously interact with real devices. This platform can serve as the basis for any CR-related research, without the need for multiple transceivers and complex integration schemes, providing unique flexibility and upgradability, supporting effortlessly the most advanced cognitive radio schemes and techniques.

References

[1] K. Qaraqe, H. Celebi, A. Gorcin, A. El-Saigh, H. Arslan, and M. Alouini, “Empirical results for wideband multidimensional spectrum usage,” in *Proc. 20th IEEE Personal, Indoor and Mobile Radio Communications, 2009*, 2009, pp. 1262–1266.

[2] V. Valenta, Z. Fedra, R. Marsalek, and M. Villegas, “Analysis of spectrum utilization in suburb environment evaluation of potentials for cognitive radio,” in *Proc. Ultra Modern Telecommunications and Workshops, ICUMT 2009*, 2009, pp. 1–6.

[3] FCC, 1985, authorization of Spread Spectrum Systems Under Parts 15 and 90 of the FCC Rules and Regulations. Federal Communications Commission. June 18, 1985. http://www.marcus-spectrum.com/ documents/81413RO.txt.

[4] Z. Jin and K. Subbalakshmi, “Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks,” in *Proc. ICC*, 2009, pp. 1–5.

[5] R. Chen, J. Park, and J. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” *IEEE J. Sel. Areas Commun*, vol. 26, pp. 25–37, 2008.

[6] A. Rawat, P. Anand, H. Chen, and P. Varshney, “Countering byzantine attacks in cognitive radio networks,” in *Proc. ICASSP*, 2010, pp. 3098–3101.

[7] W. Wang, H. Li, Y. Sun, and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks,” in *Proc. CISS*, 2009, pp. 130–134.

[8] A. G. Fragkiadakis, E. Z. Tragos, and I. G.Askoxylakis, “A survey on security threats and detection techniques in cognitive radio networks,” *IEEE Communications Surveys & Tutorials*, vol.15, no.1, pp. 428-445, First Quarter 2013.