Distributed cognitive radio architecture with automatic frequency switching

Pietro Morerio, Krešimir Dabčević, Lucio Marcenaro, Carlo S. Regazzoni
DITEN
Department of Naval, Electric, Electronic and Telecommunication Engineering
Via Opera Pia 11A 16145 Genova - Italy
{pmorerio,kresimir.dabcevic}@ginevra.dibe.unige.it {lucio.marcenaro,carlo.regazzoni}@unige.it

***Abstract*—The employment of sophisticated tools for data analysis in distributed or structurally complex systems requires the development of specific architectures and data fusion strategies in order to integrate heterogeneous information coming from the environmental sensors. Recently, intelligent sensor networks have been widely deployed for various purposes concerning both security- and safety-oriented systems. Military and civil applications ranging from border surveillance and public spaces monitoring to ambient intelligence and road safety are examples of such various applications. The architecture presented in this article is based on the Cognitive Node (CN) - a module able to receive data from the sensors, process it in order to find potentially harmful or anomalous events and situations and, in some cases, to interact with the environment itself or contact the human operator. The cognitive model was studied and exploited, focusing on the analysis and decision blocks which represent the crucial phases for assessing potentially unsecure/unsafe events and/or situations. The scalability of the model with regards to different application domains was investigated during the research activity. Proposed results show the capability of the given architecture for analysis and assessment of the occurring interactions, with the goal of maintaining proper security/safety levels in the monitored environment.**

I. Introduction

The problem of spectrum scarcity has been one of the central domains of interest within the radiocommunication research community for some time now. With many new spectrum-demanding radio-based services, such as video broadcasting, continuously penetrating the market, finding ways to increase the spectrum usage efficiency has become paramount. Cognitive radio (CR) represents a technological breakthrough that will - among other things - deal with this matter specifically. Cognitive radio can be described as an intelligent and dynamically reconfigurable radio that can adaptively regulate its internal parameters as a response to the changes in the surrounding environment. Namely, its parameters can be reconfigured in order to accomodate the current needs of either the network operator, spectrum lessor, or the end-user.

More often than not, cognitive radio is being defined as an upgraded software-defined radio (SDR) (a radio in which, opposed to the traditional radio, some or all of the modules can be controlled sofware-wise), with learning mechanisms based on some of the machine learning techniques, and potentially also equipped with smart antennas, geolocation capabilities, biometrical identification, etc. (e.g., see [1]).

However, it is exactly these newly-introduced cognitive capabilities that make cognitive radios - in addition to the security issues they face due to their wireless networks in general - susceptible to a whole new set of potential security issues and breaches. One of the most common security attacks launched against CRs is the Primary User Emulation Attack [2], where an impostor wireless node tries to emulate the behavior of the licensed primary user with the goal of disturbing the opportunistic spectrum usage techniques implemented by cognitive radio nodes. Spectrum Sensing Data Falsfication Attack is another attack targeting the cognitive radio network's physical layer, and is unique to cognitive radio networks that use one of the collaborative spectrum sensing schemes - reliability of the collaborative spectrum sensing can be severely degraded by providing faulty observations by one or more of the network's nodes. Attacks targeting higher levels (MAC/transport/combination of layers) are also existent namely, congestion-oriented attackers use flooding techniques in order to cause Denial of Service (DoS) attacks, whereas jamming-oriented attackers rely on creating interference to achieve DoS.

A smart jammer [3] is a particular type of attacker that is able to scan the entire spectrum and selectively jam specific channels, thus causing anomalous spectrum usage and actually interfering with dynamic spectrum access techniques. Detecting these kinds of security issues within cognitive radio network ([4]) is not an easy task, and often requires sophisticated approaches and algorithms. Establishing such appropriate measures and algorithms, focusing specifically on the security, privacy and dependability (SPD) of embedded systems, was one of the main objectives of the pSHIELD project ([5]) whereas developing them is the focus of its successor - the ongoing nSHIELD project ([6]). Within those projects, we have developed a general purpose distributed cognitive architecture that can efficiently be used for cognitive radio security-related applications. The architecture is built on several processing nodes that are able to fuse data coming from deployed sensors at different abstraction levels. By detecting wireless nodes moving in the monitored environment, it is possible to assess the overall situation of the environment and predict potentially dangerous events such as the presence of a smart jammer. The cognitive node is also able to communicate with other nodes, potentially leading to the modification of

some transmission parameters in order to avoid jammer-caused problems. Several parts of the proposed architecture have been ported onto an ARM-based embedded processor. The effectiveness of the proposed scheme is demonstrated by extensive simulations.

The remainder of this paper is organized as follows: section II describes the principles of cognitive systems, while the proposed demonstrator is illustrated and simulation results are given and discussed in section III. Section IV concludes the article, giving a brief description of the future work and challenges.

II. Cognitive systems

Two limitations of the standard elaboration modules in intelligent systems are represented by their passivity and the inability to learn based on experience.

Cognitive systems can overcome these limitations by the means of the cognitive cycle (sensing-analysis-decision-action). Cognitive systems indeed implement a model which imitates the brain functionalities and are not only able to draw correct conclusions in different situations, but are also able to come up with a decision in order to adapt to the situation, and consequently act ([7]). A cognitive system has the capability of interacting in a closed cycle with the outside world by the means of the actuators present in the environment. The cognitive system has an internal model which describes the actuators related to itself and the action they can make towards the environment (embodied cognition) ([8]).

A. Cognitive model

Cognitive systems are based on a neurophysiological model of reasoning and awareness ([9]). In this model, a cognitive entity is described as a complex system which is able to learn incrementally - on the basis of experience - relations between themselves and the external world. Neuroscientific conceptualization of cerebral human functions defines two specific devices, called proto-self and proto-core, which are devoted to monitoring and management of the internal state of the entity and of the external world respectively. The possibility of gaining access to its own internal state (self-consciousness) for the cognitive entity is as necessary as the ability of analyzing the environment. According to this model, the sensors available to a cognitive entity can be divided into endo-sensors (or proto sensors) and eso-sensor (or core sensors), depending on whether they are used for internal or external states monitoring.

The behavior of a cognitive entity interacting with the world is described by the cognitive cycle and can be divided (Figure 1) in four fundamental steps: Sensing, Analysis, Decision, Action. These steps represent an infinite deterministic sequence.

Therefore, the conceptual architecture of a cognitive entity is made of four logical blocks (Figure 1):

- **Sensing**: cognitive system constantly gets information about the core- and self-states by means of endo- and eso-sensors.

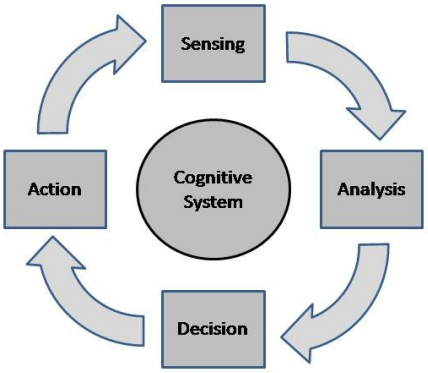


Fig. 1. The cognitive cycle

- **Analysis**: data coming from the sensors is fused in order to obtain a common description of the external world as well as the internal state of the cognitive system. Input data is then analyzed to detect events, which can in turn be either proto events (ϵ^P) - relative to significant changes in the internal state of the system, or core (ϵ^C) - relative to changes in the external world. From such data, cognitive entity is able to create a model of probability distributions of proto and core events, $p(\epsilon_t^P|\epsilon_{t-1}^P)$ and $p(\epsilon_t^C|\epsilon_{t-1}^C)$. This model (first order neural pattern) does not account for the possible interactions between the core and proto events, and can be regarded as a pair of Dynamic Bayesian Networks (proto-DBN and core-DBN).
- **Decision**: based on the experience of the cognitive system and the analysis of the current internal and external states $\mathbf{X}_p$ and $\mathbf{X}_c$, the system selects the most appropriate strategy S_t for achieving the desired system state $\mathbf{X}_p, \mathbf{X}_c$.
- **Action**: this module refers to the active interaction of the system towards the surrounding environment: an appropriate action a_i is selected based on the strategy S_t that was chosen marked as the most appropriate during the previous step.

III. The demonstrator and simulation results

The demonstrator deals with the system architecture of Dynamic Spectrum Management (DSM)-capable cognitive radio networks. We will try to focus on practical considerations of such architectures. In particular, we will concisely describe the architecture of a single cognitive radio terminal and - in more details - the architecture of DSM-capable systems, with particular emphasis on DSM-capable Tactical Communication Systems (TCS). The necessity of having DSM capabilities for the current tactical military systems is investigated as well. In order to incorporate such capabilities in a wireless system, our main focus will be on the management of radio parameters (e.g., transmit-power, carrier-frequency, and modulation strategy); network topology; network performances, as well as the issues related to the security of the system, taking into account all of the possible inter-radio interactions, including those with smart jammers.

One of the possible threats to the spectrum sensing process is the previously mentioned data falsification attack. For combatting SSDFAs, we consider a two-layer defense mechanism: a) authentication at the first layer in order to prevent replay or false data coming from outside of the network, and b) a data fusion scheme that is robust against spectrum sensing data falsification.

The anti-jamming capability of a DSM-capable cognitive radio network is another relevant related topic. A jammer is a device that intentionally generates RF signals to disrupt the normal operation of a communication system. There are many different types of jammers depending on their allocation, ranging from disrupting the signal receipt at the target receivers, to more sophisticated ones, such as deceiving the targets into accepting false information. These highly sophisticated and adaptable ones, expected to be found in the future cognitive radio networks, are of particular interest for our research. Smart jammers can typically consist of three major components:

- a spectrum sensor, which senses and locates target's physical channel;
- a spectrum analyzer, which analyzes the sensed spectrum data and, combinining it with the prior knowledge of the target channel, consequently devises an action;
- a radio transmitter, which is dedicated to radiating jamming signals.

In this demonstrator, a cognitive radio node is implemented as a set of C/C++ interacting modules running on an IGEPv2 - a compact ARM-based industrial processor board. The cognitive node is able to sense signal strength of detected mobile entities and - by comparing the received signal strengths - has the ability to detect jammers within the monitored environment. Implemented prototype is able to deal with fixed and mobile jammers - after a jammer is detected, the cooperative mobile entity automatically modifies its operating frequency.

The scenario consists of a number of entities (agents) carrying a mobile device which is able to transmit and receive data at 3 different frequencies (namely 900, 1800 and 1900 MHz) to a centralized control center. The agents move randomly throughout the jamming-polluted environment. The jammers can be either fixed or mobile, and their emitted signal strength follows the Rayleigh distribution with fixed parameters. Fixed jammers' positions and characteristics are stored in an XML file, which is loaded in the setup stage together with the map of the ground. An example of a scenario with 2 moving agents (Agent1 and Agent2) originally transmitting at the frequency of 1800 MHz, and three fixed jammers (J0 - J3) jamming at 800 MHz, 800 MHz and 1800 MHz respectively, with their respective radii of sensing and influence is depicted in Figure 2(a). The agents periodically send a single radio data to the control center, where the running cognitive node receives and processes it.

Radio data sent by an agent contains the following information:

- *Position of the agent (x,y) on the mapped ground*: this is generated by the trajectories simulator. It simulates a GPS sensor on the mobile device. If video monitoring of the ground area is available, positioning data coming from the tracker can potentially be fused with the GPS data in order to obtain a better position estimation.
- *Frequency of the transmission*: initial transmission frequency can be chosen at the beginning of the simulation, whereas information of the updated frequencies are sent in every timeframe.
- *Power of the transmitted signal*: fixed.
- *Possibly detected jammers' estimated power*: each jammer has a typical radius (coded in the XML configuration file) of influence, inside which the agent can estimate its power (knowing that the signal strength follows the Rayleigh distribution).
- *IDs of the possible neighboring agents* (within a fixed sensing radius).

We can also look at a slightly different scenario by introducing a moving jammer: now, an additional agent (Agent3), carrying a jamming device, has been added to the scene. Besides disturbing communication at its operating frequency within its jamming radius, it also transmits spurious data to the cognitive node regarding its position. A scenario with 2 moving agents transmitting at the frequency of 1800 MHz and one Jammer transmitting at the same frequency, with their respective radii of sensing and influence is depicted in Figure 2(b).

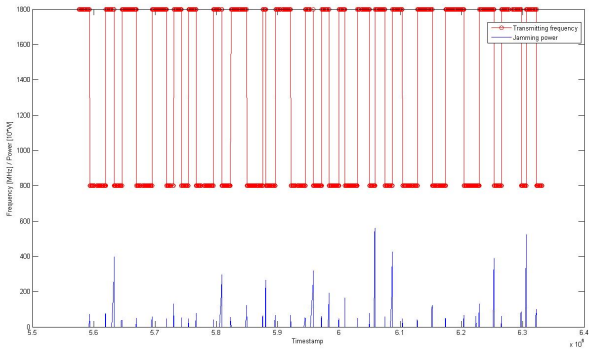
(a) Scenario with two agents and three fixed jammers

(b) Scenario with mobile jammer (intruder)

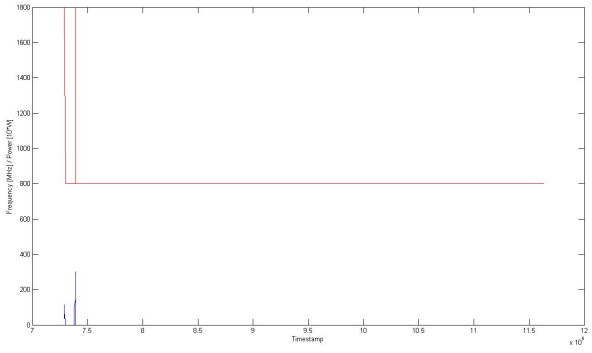
Fig. 2. Fixed and mobile jammers scenario

Frequency switching process for one of the agents (Agent1) as a function of time, and depending on the jamming power of the nearby jammers is given in Figure 3(a). The same process for both agents (Agent1 and Agent2) for the modified (mobile-jammer) scenario is given in Figure 3(b). As can be seen, in this case the frequency switching only occurs once for each of the agents: since mobile jammer doesn't have the capability

of jamming multiple frequencies, there is no reason for agents 1 and 2 to deviate from their newly-set frequencies once they start transmitting at frequency not influenced by the malicious agent.



(a) Scenario with two agents and three fixed jammers



(b) Scenario with mobile jammer (intruder)

Fig. 3. Frequency switching depending on the jammer power

The radio data reception represents, from the node point of view, the "sensing" stage of the cognitive cycle. The agents' mobile terminals are equipped with sensors which monitor the environment, sending a radio survey (radio sensors) and positioning (GPS sensor) information to the cognitive node.

The cognitive node - acting as a data fusion center - then analyzes all the information received from each agent. For each agent, the signal-to-noise and distortion ratio (SINAD) of the received data packet is computed. Also, agents' relative positions are compared, and by the means of the voting algorithm, rankings are assigned to each agent's ID. Then, intruder's position and ID are worked out.

In the decision stage, the SINAD datum is compared to an acceptable (fixed to $10dB$) threshold. If the communication with an agent under the jamming influence proves to be below the acceptable threshold, a suitable strategy ST is chosen in order to schedule a change in the transmit frequency.

The "action" stage leads to the change in the state of the system. As was previously explained, this module implements the active interaction of the system towards the surrounding environment or towards itself: the action of changing frequency is selected based on the strategy ST chosen during the previous step.

Hence, detection of the intruder does not trigger a decision and a subsequent action in the cognitive cycle. Instead, the information relative to the malevolent agent is transmitted to the third party agent, which in real-life application could, for example, display data on the mobile devices, thus leaving the decision step under human control. Alternatively, a learning-based-on-experience strategy could be deployed within the cognitive node in future perspective.

IV. Conclusions and Future Work

A distributed architecture for cognitive systems was presented. The architecture was implemented as a set of C/C++ interacting modules that are able to run on standard PCs, as well as on embedded architectures. The cognitive radio node is able to receive measured spectrum-related data from the wireless nodes, detect potential attacker nodes, and modify transmission parameters of trusted nodes in order to avoid jammer-caused disturbances.

Future work will focus on improving both the attacker's capabilities, such as adding the ability to alternate its transmission frequency and transmission power, and appropriate security countermeasures by the defense system, with special focus on developing learning capabilities based on experience.

Acknowledgements

This work was developed within nSHIELD project (http://www.newshield.eu) co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-programme SP6) focused on the research of SPD (Security, Privacy, Dependability) in the context of Embedded Systems.

References

[1] L. Bixio, L. Ciardelli, M. Ottonello, M. Raffetto, C.S. Regazzoni, S.S. Alam, and C. Armani, "A transmit beamforming technique for mimo cognitive radios," in *SDR'11 - The Wireless Innovation Forum Conference on Communications Technologies and Software Defined Radio*, Brussels, Belgium, Jun 2011.

[2] Husheng Li and Zhu Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems - part ii: Unknown channel statistics," *IEEE Transactions on Wireless Communications*, vol. 10, no. 1, pp. 274–283, 2011.

[3] C. Sorrells, P. Potier, Lijun Qian, and Xiangfang Li, "Anomalous spectrum usage attack detection in cognitive radio wireless networks," in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, nov. 2011, pp. 384 –389.

[4] Timothy X. Brown and Amita Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment," *Mob. Netw. Appl.*, vol. 13, no. 5, pp. 516–532, Oct. 2008.

[5] pSHIELD Consortium, "Pilot shield," http://www.pshield.eu/, June 2010.

[6] nSHIELD Consortium, "New shield," http://www.newshield.eu/, Jan. 2012.

[7] Alessio Dore, Matteo Pinasco, Lorenzo Ciardelli, and Carlo S. Regazzoni, "A bio-inspired system model for interactive surveillance applications," *JAISE*, vol. 3, no. 2, pp. 147–163, 2011.

[8] M. L. Anderson, "Embodied cognition: A field guide," *Artificial Intelligence*, vol. 149, no. 1, pp. 91 – 130, 2003.

[9] Antonio Damasio, *The Feeling of What Happens: Body and Emotion in the Making of Consciousness*, Harvest Books, October 2000.