ERCIM NEWS

European Research Consortium
for Informatics and Mathematics
www.ercim.eu

Special theme: Unconventional Computing Paradigms

Also in this issue:

requirements, and is influencing the design and implementation decisions.

Figure 1 summarizes the main concept of PANDORA. A group of trainees, from different agencies (eg, Civil Defence, Health, Fire Service, Police, Transportation) access the training system. If some authorities are not present, they are simulated through Non Player Characters. Each trainee feeds personal data to the PANDORA kernel, which gathers this information to build a user model (Behavioral Module). On the basis of this model, the system synthesizes personalized training paths (Behavioral Planner). The output of this process is passed to a second module (Crisis Planner), which uses both the Behavioral Module indications and knowledge of the chosen scenario to plan sequences of stimuli appropriate for the group (information shared among all trainees)

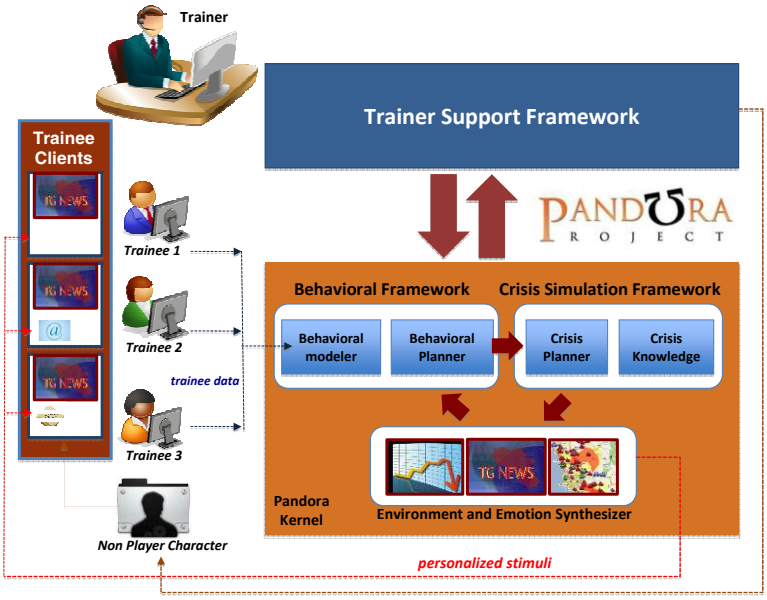

Figure 1 The PANDORA system architecture

and the individual trainees (information tailored to induce the "right level of stress").

The plan is then passed to the Environment and Emotion Synthesizer, responsible for an effective rendering of the various stimuli. A separate module (Trainer Support Framework) allows trainers to control the training session and dynamically adjust the stimuli based on their experience.

PANDORA uses timeline-based planning technology which allows for rich domain modelling and uses both temporal and resource constraints. A timeline can be seen as a stepwise constant function of time. Specifically it is an ordered sequence of values holding on subsequent temporal intervals. This approach has been used both in the Behavioural and the Crisis Framework.

In the first case some psycho-physiological trainee features, shown to influence human behaviour under crisis, are modelled and updated during training as timelines. On the basis of this model, the Behavioural Planner synthesizes goals for the Crisis Planner. The Crisis Planner creates training storyboards, sets of "events" communicated to the trainees (eg, a news video from the crisis setting, a phone call or e-mail from an operational or tactical manager). Additionally, the Planner "reacts" to trainees' strategic decisions, triggering subequent events to continue the session.

The overall system empowers the trainer with a new means for training people. Indeed the suggested crisis stimuli and the behavioural analysis are presented to the trainer to influence at any moment the training session, in perfect line with a mixed-initiative style.

Links:
http://www.pandoraproject.eu/
http://epcollege.com/
http://pst.istc.cnr.it/

Please contact:
Amedeo Cesta, ISTC-CNR, Italy
E-mail: amedeo.cesta@istc.cnr.it

Keith Strickland - EPC, UK
keith.strickland@cabinet-office.x.gsi.gov.uk

Security and Resilience in Cognitive Radio Networks

by Vangelis Angelakis, Ioannis Askoxylakis, Scott Fowler, David Gundlegård, Apostolos Traganitis and Di Yuan

After more than a decade of research, system security and resilience is now the major technological barrier for the Cognitive Radio (CR) to be adopted by the telecommunication industry. New ideas are required to make CR networks secure and robust against attacks taking advantage the inherent characteristics of the CR functionality. This work explores key points that urgently need to be addressed.

Cognitive radio (CR) is a term with many possible meanings in the telecommunications literature of the past decade. Most commonly, a cognitive radio device is based on a software-defined radio (SDR), and has an adjustable front-end, which allows it to tune on different frequencies, power levels and modulation schemes. The SDR infrastructure has a programming interface that enables these configuration options. These, in conjunction with the context of operation (radio interference and noise, traffic demand, mobility levels, element status, location, etc) are made available to a decision-making entity, which selects the best configuration by solving an optimization problem with respect to some objective function. Further input is contained in a system knowledge base that codes the contexts encountered and maps them to specific radio configurations that can be used. This mapping can be done through a reasoning engine which is essentially a set of logical inferring rules (policies) and "reasons" (i.e. searches) for a proposed set of actions that will manipulate the current state of the knowledge base in an

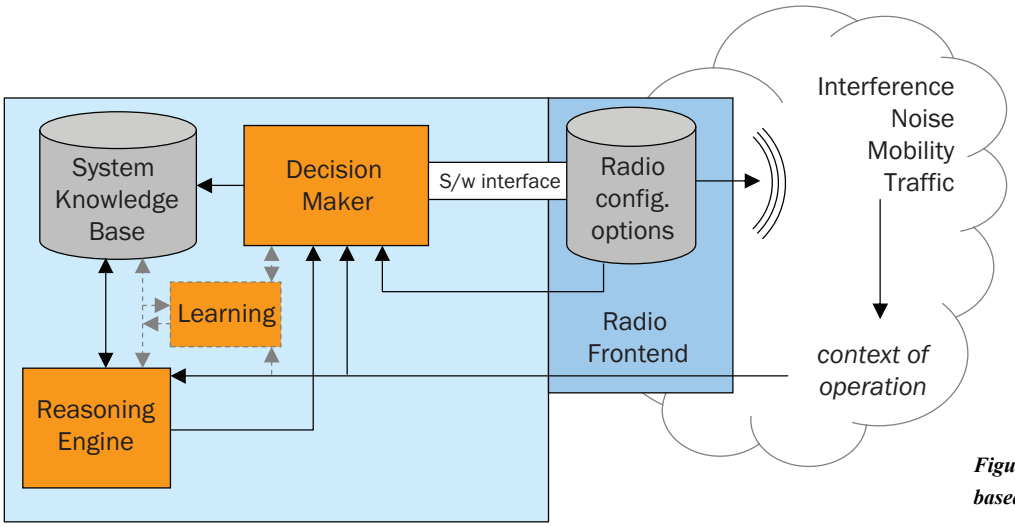

Figure 1: Components of a SDR-based Cognitive Radio.

optimal way. In principle, the CR functionality may also include a learning engine making it capable of starting with no policies, and by utilizing a variety of classic Artificial Intelligence (AI) learning algorithms identify which configuration will work optimally in the current and future contexts.

While CR devices are built with components that have been well-established in the telecommunications and computer science disciplines, the existing approaches to provide robustness and effective security for a network of CR devices are inadequate. Due to the particular characteristics of the CR systems, new types of attack are possible and some of the well-known types increase in complexity. Therefore, new ideas are needed to make CR networks secure and robust against specific attacks, especially against those that are inherent to the CR functionality.

Specifically, sample attacks can target the inputs considered for the formation of the CR networks and the respective optimization problem, for instance attacks might compromise the accuracy of the context information sensed or the set of candidate nodes that may be involved in the network. One of the key features of cognitive radio is that sensory manipulation can lead to knowledge manipulation, meaning that malicious actions in the present can affect the radio performance in the future. Other attacks can target the outputs describing the CR network that should be formed even under unharmed inputs, eg, a set of nodes that should be involved, configurations that should be selected, etc. Finally, as in all wireless networks, attacks can be designed to lead the client devices to configurations that are inefficient in terms of energy and make them run out of batteries.

There is, therefore, the need for comprehensive and energy efficient mechanisms to discourage, identify and mitigate the attacks at all phases of the cognitive cycle, in order to obtain CR systems that are trustworthy, efficient and dependable. Furthermore, in this scope there is need for a new systemic evaluation of the robustness of a CR system, in order to set the requirements and expectations for a resilient CR network from a security viewpoint.

The targets of this joint work are to initially identify the threats at the different layers and to classify the major topics, such as jamming, sensory manipulation, belief manipulation, routing, etc , for each layer.

Further on we aim to develop new mechanisms for detecting, isolating and expelling misbehaving insiders. Such malicious nodes may have all the credentials provided by an "off the shelf" security solution as the ones proposed to be applied in IEEE 802.22. This therefore requires the detection of abnormal secondary user operation through pattern analysis and node cooperation, since the feedback from the CR devices will enhance the efficiency required for such an Intrusion Detection System (IDS).

Improving sensory input can reduce the exploitability of cognitive radios in a cross-layer fashion. For example, if the CR could identify the difference between interference and noise, they would distinguish between natural and malicious RF events. Identification and quantification of potential gains from the interference identification is important in order to define more robust CR MAC policies. Furthermore, in a distributed environment, a network of cognitive radios can fuse sensor data to improve the quality of input for the cognitive engine. Such techniques should be designed with small information exchange requirements in order to be energy efficient, keeping in mind that the client CR devices will be battery operated.

This project is a joint effort by the Mobile Telecommunications group of the Department of Science and Technology in Linköping University and the Institute of Computer Science of the Foundation for Research and Technology-Hellas (FORTH-ICS).

Please contact:
Vangelis Angelakis,
Mobile Telecommunications, ITN-LiU, Sweden
Tel: +46 11 363005
E-mail: vangelis.angelakis@liu.se

Ioannis G. Askoxylakis,
FORTH-ICS, Greece
Tel: +30 2810 391723
E-mail: asko@ics.forth.gr

ERCIM
European Research Consortium for Informatics and Mathematics

ERCIM – the European Research Consortium for Informatics and Mathematics is an organisation dedicated to the advancement of European research and development, in information technology and applied mathematics. Its national member institutions aim to foster collaborative work within the European research community and to increase co-operation with European industry.

ERCIM is the European Host of the World Wide Web Consortium.

AARIT
Austrian Association for Research in IT
c/o Österreichische Computer Gesellschaft
Wollzeile 1-3, A-1010 Wien, Austria
http://www.aarit.at/

CNR
Consiglio Nazionale delle Ricerche, ISTI-CNR
Area della Ricerca CNR di Pisa,
Via G. Moruzzi 1, 56124 Pisa, Italy
http://www.isti.cnr.it/

Crcim
Czech Research Consortium
for Informatics and Mathematics
FI MU, Botanicka 68a, CZ-602 00 Brno, Czech Republic
http://www.utia.cas.cz/CRCIM/home.html

CWI
Centrum Wiskunde & Informatica
Centrum Wiskunde & Informatica
Science Park 123,
NL-1098 XG Amsterdam, The Netherlands
http://www.cwi.nl/

fonds national de la recherche
Fonds National de la Recherche
6, rue Antoine de Saint-Exupéry, B.P. 1777
L-1017 Luxembourg-Kirchberg
http://www.fnr.lu/

FWO
Egmontstraat 5
B-1000 Brussels, Belgium
http://www.fwo.be/

FNRS
rue d'Egmont 5
B-1000 Brussels, Belgium
http://www.fnrs.be/

FORTH
Foundation for Research and Technology – Hellas
Institute of Computer Science
P.O. Box 1385, GR-71110 Heraklion, Crete, Greece
http://www.ics.forth.gr/

Fraunhofer IUK-TECHNOLOGIE
Fraunhofer ICT Group
Friedrichstr. 60
10117 Berlin, Germany
http://www.iuk.fraunhofer.de/

INRIA
Institut National de Recherche en Informatique
et en Automatique
B.P. 105, F-78153 Le Chesnay, France
http://www.inria.fr/

IUA
Irish Universities Association
Cumann Ollscoileanna Éireann
Irish Universities Association
c/o School of Computing, Dublin City University
Glasnevin, Dublin 9, Ireland
http://ercim.computing.dcu.ie/

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and
Electrical Engineering, N 7491 Trondheim, Norway
http://www.ntnu.no/

PEG
PORTUGUESE ERCIM GROUPING
Portuguese ERCIM Grouping
c/o INESC Porto, Campus da FEUP,
Rua Dr. Roberto Frias, nº 378,
4200-465 Porto, Portugal

Universitas Varsoviensis
PLERCIM
Universitas Wratislaviensis
Polish Research Consortium for Informatics and Mathematics
Wydział Matematyki, Informatyki i Mechaniki,
Uniwersytetu Warszawskiego, ul. Banacha 2, 02-097 Warszawa, Poland
http://www.plercim.pl/

Science & Technology Facilities Council
Science and Technology Facilities Council,
Rutherford Appleton Laboratory
Harwell Science and Innovation Campus
Chilton, Didcot, Oxfordshire OX11 0QX, United Kingdom
http://www.scitech.ac.uk/

SpaRCIM
Spanish Research Consortium for Informatics and Mathematics
Spanish Research Consortium for Informatics and Mathematics,
D3301, Facultad de Informática, Universidad Politécnica de Madrid,
Campus de Montegancedo s/n,
28660 Boadilla del Monte, Madrid, Spain,
http://www.sparcim.es/

Swedish Institute of Computer Science
SICS
Swedish Institute of Computer Science
Box 1263,
SE-164 29 Kista, Sweden
http://www.sics.se/

SARIT
Swiss Association for Research in Information Technology
c/o Professor Daniel Thalmann, EPFL-VRlab,
CH-1015 Lausanne, Switzerland
http://www.sarit.ch/

MTA SZTAKI
Magyar Tudományos Akadémia
Számítástechnikai és Automatizálási Kutató Intézet
P.O. Box 63, H-1518 Budapest, Hungary
http://www.sztaki.hu/

VTT
Technical Research Centre of Finland
PO Box 1000
FIN-02044 VTT, Finland
http://www.vtt.fi/

Order Form

If you wish to subscribe to ERCIM News ***free of charge*** *or if you know of a colleague who would like to receive regular copies of ERCIM News, please fill in this form and we will add you/them to the mailing list.*

Send, fax or email this form to:

ERCIM NEWS
2004 route des Lucioles
BP 93
F-06902 Sophia Antipolis Cedex
Fax: +33 4 9238 5011
E-mail: office@ercim.eu

Data from this form will be held on a computer database. By giving your email address, you allow ERCIM to send you email

I wish to subscribe to the

☐ ***printed edition*** ☐ ***online edition (email required)***

Name:

Organisation/Company:

Address:

Postal Code:

City:

Country

E-mail:

You can also subscribe to ERCIM News and order back copies by filling out the form at the ERCIM Web site at http://ercim-news.ercim.eu/