Multi-sensor cognitive-based approach to critical infrastructure protection

L. Ciardelli[1], L. Bixio[1], M. Ottonello[1], M. Cesena[2]
& C. S. Regazzoni[1]
[1] *Department of Biophysical and Electronic Engineering, University of Genoa, Genoa, Italy*
[2] *Selex Communications S.p.A, Genoa, Italy*

Abstract

Critical Infrastructure Protection (CIP) represents a particularly relevant issue worldwide. Moreover, the evolution of technologies at the disposal of criminal activities is leading to an increasing need for a technological basis and relevant knowledge to improve security capabilities. Especially, more work has to be done in defining a security architecture that takes into account cascading effects, inter and intra dependencies, distributes the intelligence in the infrastructure to increase its robustness, trustworthiness and resilience. According to this statement, an innovative situation awareness and assessment based approach for the monitoring of Critical Infrastructures is proposed. In particular, based on recent studies on artificial cognitive systems, we explore the concepts for designing interactive, adaptable and intelligent multi sensor surveillance systems able to react to situations in a preventive and manageable way. To reach this goal, in this paper we emphasize that innovative strategies could be based on the integration of heterogeneous sensing devices, such as distributed cognitive radio sensors for communication and monitoring and a network of smart cameras for the interpretation of interactions and events.

1 Introduction

In the last few years, our society has been threatened by the continuous rise in acts of terrorism. Therefore, CIP has become a general label for a range of activities undertaken jointly by governments and operators of key locations, facilities and systems to ensure they are adequately managing risk. These initiatives cover two

WIT Transactions on the Built Environment, Vol 108, © 2009 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE090081

main categories:

- *critical infrastructure assets* - those assets or systems deemed more likely to be targeted because of the downstream impact of a successful attack, or where the consequences would be intolerably severe, or some combination of the two;
- *places of mass gathering* - those types of sites where large numbers of people congregate (e.g. mass scale sport events as Olympic Games or high relevance international meetings, such as G8).

Moreover, it appears that no clear and scalable security model exists for big critical infrastructures. Existing models of such systems are vague and there are no methodologies for understanding the behaviour of complex systems. Especially, in the literature it is emphasized how the modelling and analysis of these systems are a challenge because of their large-scale, non-linear, and time-dependent behaviour [1–3]. As well, research activities in homeland security applications [4, 5], which represent a major concern for governments worldwide, highlight that only a few information and communication technology components have been developed to meet high assurance standards.

According to presented issues, smart multi-sensor surveillance systems could be applied as an innovative and effective means of maintaining public areas under secure and safe conditions. The role of such systems is twofold. Firstly, they provide an automatic interpretation of scenes; secondly, they are able to understand and predict the actions and interactions of the observed objects based on the information acquired by sensors. In the literature, several solutions have been proposed to create efficient and robust system architectures. In [6] two examples are presented, referring to an airport and an oil refinery plant, indicating how computer vision technology is effective for asset protection, perimeter monitoring and threat detection. In [7] the impact of distributed processing and innovative communication techniques on third generation surveillance systems (3GSS) has been investigated and evaluated. In particular, a solution able either to increase flexibility and reconfigurability of the system or to optimally allocate processing and bandwidth resources has been proposed. The work presented in [8] explores the introduction of smart features for real-time video analysis, active cameras and long-term pattern analysis. According to the authors, particular relevance resides in the capability of such systems to curtail personnel visual monitoring tasks, returning automatically alarm signals. As well, in [9, 10] the capability of Wireless Sensor Networks (WSN) to collect information from the environment in a distributed manner has been provided revealing their usefulness from a civil and military viewpoint (e.g. surveillance, environmental monitoring, manufacturing, business asset management, transport automation, security and health-care).

Thus, based on multi-modal data fusion techniques [11, 12], an innovative approach for the design of distributed sensor networks for surveillance applications can take advantage of this significant recent body of research on cognitive systems and from interdisciplinary studies coming from the brain neurosciences field [13]. As a matter of fact, the capabilities of flexibility, intrinsic in cognitive systems (CS), are enormously attractive in applications where self-awareness, self-

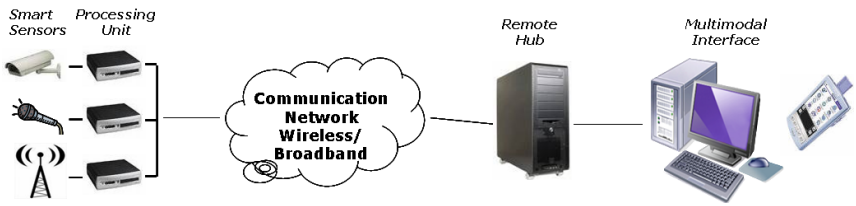

Figure 1: Architectural example of smart multi-sensor surveillance systems.

adaptation and capability of learning from experience features are required. This article explores the concepts of embodied cognition and the use of video-radio analysis to provide an innovative approach to comprehensive situation awareness for CIP. In Section 2 a description of cognitive models is presented. Section 3 focuses on capabilities of cognitive-based video and radio sensors while in Section 4 a simulated application scenario and promising preliminary results are presented.

2 Cognitive-based approach

In recent years, neurosciences provided better insight and evidence of human intelligence mechanisms exploiting the strict relationships between mind processes and body of intelligent organisms. Therefore, taking inspiration from such processes, a key issue of an innovative bio-inspired CIP approach is defining adaptive and evolutionary architectures based on embodied cognition paradigms [14]. Such a system will be characterized by the ability of improving its behaviour through the experiences directly lived or only observed. Bio-inspired schemes provide natural interactions with human users, complete transparency, easy implementation at every level of the communication system architecture and intelligent support to everyday life. In particular, from the work of the neurophysiologist Damasio [15], the basis to model the system as a cognitive entity are drawn to enable the intelligent and adaptable relationship with users and the environment. The first aspect to be considered is the distinction between what is internal and what is external with respect to the entity to be modelled, since, according to Damasio, self consciousness arises from the conscious interaction with external entities. In this way the system is intended to be provided with context awareness and "conscious" reasoning capabilities. The brain devices that are devoted to supervise and manage the internal state of the organism and the relation with external entities are respectively called proto-self and core self. The proto-self computes the information regarding the organism's internal state gathered by the proto sensor. Similarly the core sensors analyze the external world and provide data to the core self. According to this, the internal and external states of the entity will be named proto state and core state. The common shared model for describing the behaviour of a cognitive system is the so-called Cognitive Cycle (see Figure 2) which is composed by four main characteristics:

- Sensing: the system has to continuously acquire knowledge about the interacting objects and about its own internal status, sensing is a passive interaction component;
- Analysis: the perceived raw data need an analysis phase to represent them and extract interesting filtered information;
- Decision: the intelligence of the system is expressed by the ability to decide for the proper action, given a basic knowledge, experience and sensed data;
- Action the system tries to influence its interacting entities to maximize the functional of its objective, action is an active interaction component in relation to decision.

The learning phase is continuous and involves all the stages (within certain limits) of the cognitive cycle. To learn interactions, an algorithm, called Autobiographical Memory, has been developed (see [16]) and exploited to model how the human brain stores causal relationships with external entities and how it uses this information to predict near future events. The capability of an entity of predicting the near future and of reacting in a proactive manner to interacting users actions represents a key feature of a distributed surveillance system. According to cognitive paradigm, methods for the representation, organization, learning from experience and usage of knowledge allow a system to anticipate the state evolution and to plan, consequently, appropriate counteractions to maintain the security standard of the monitored environment. Therefore, referring to previously highlighted issues, a cognitive-based approach aims at providing the system capabilities of either directly acting on the environment itself or to communicate and cooperate with human agents to perform indirect anticipatory/corrective actions.

3 Multi-sensor cognitive surveillance

The physical architecture of a cognitive system for surveillance, inspired by the concepts expressed in Section 2 is composed by three main components:

- sensors: a bunch of sensors can be used in a cognitive surveillance system to observe both the elements constituting the environment (e.g. doors, windows, etc.) and the presence of objects of interest in the monitored area. Examples of such devices are cameras, IR sensors, volumetric sensors, radio (e.g. WLAN, Bluetooth, etc.) signal analyzers.
- server and processing units: the server is the core of the system where the analysis of the signals acquired is performed, the decision phase is accomplished using the learned information and the actuators or communications devices are driven.
- actuators: the system can be provided of actuators and communications devices as doors and windows locks, palms, speakers, etc. to directly affect the environment and the subjects present in it. These devices can be connected through either wired connections (e.g. LAN, Firewire IEEE 1394, etc.) or wireless ones (e.g. WLAN, Bluetooth, etc.) to achieve a large degree of flexibility design.

Figure 2: Cognitive cycle.

From a general point of view, the proposed system permits to represent two different aspect of the intelligence in the Information and Communication Technology (ICT) field: the *Ambient Intelligence* (AmI) [17] and the *Cognitive Radio* (CR) [18]. In particular, AmI solutions regard the development of context-aware applications and the capability of surveillance systems of interacting both with cooperative operators and the environment. On the other hand, the CR paradigm allows to guarantee adaptability and flexibility to the system, together with the capability of reacting to unexpected or unforeseen situations. The design of the proposed heterogeneous surveillance framework exploits together the AmI and the CR paradigm through a network of smart cameras and signal analyzer sensors. This architecture intend to dynamically combine the decision and learning capabilities of nodes in order to face anomalous situations guiding directly operators. In this context, dysfunctional behaviors are represented by actions carried out by intruders that operate against the system to create threats to environment security. Therefore, in case of anomaly, each node communicates with the control station and with other nodes providing information about the environment and dynamically alerting and supporting operators according to the changes related to previous actions. The most relevant difference, with respect to other existing system, is the augmented capability of each node of analyzing and controlling tough situations in an autonomous but manageable way in order to allow the operators to take the final decision.

3.1 Video and radio information fusion

The proposed distributed sensor network architecture is based on a cooperative strategy where the intelligent entities collaborate to reach a common goal. For instance, let consider a situation where the sensors that consigned the network have to locate and identify a possible intruder. Each cognitive terminal (e.g. a smart camera or a signal analyzer sensor) needs information both on the physical situation of the companion terminals inside the environment and on their behavioral model. Let us suppose that every terminal has the same behavioral model (i.e. guided by the same cognitive cycle). The required knowledge to perform a correct identification will be given by:

- The information about the space surrounding the sensor itself and the temporal set of positions assumed by the terminal during its route (if they are moving sensors).
- The information about the environment i. e. the knowledge about the physical/ statistical interaction characteristics of the entities present in the environment (included their positions and their behavioral models). In particular, the information is related to the position and to the behavior of the other cooperative terminals, are of great importance.
- The embodied knowledge, composed by all the functions that constitute the cognitive cycle and all the embedded information required for performing it.

Referring to the previously introduced scenario it is worth to highlight the discrimination between terminals (cognitive or not) which do not cooperate and cooperative terminals. Cooperation between the entities (signal analyzers and cameras) involves the usage of different analysis and decision algorithms. This fact has a direct impact on the information stored in the memory regarding the analysis and the decision phase. Therefore, it is possible to distinguish between:

- Configuration with fusion.
- Configuration without fusion.

In the first case the decision makers transmit their decision, a local one, to a fusion center which has to take the correct decision for the entire distributed sensor system (centralized configuration). The second case is referred to a parallel decision network without fusion; in this case it is employed a decentralized (or distributed) approach well suited to CR and AmI paradigms. Concerning last case, that is the object of our study, we have developed Data Exchange techniques where each device is provided with multiple information used by the device to take its decision, knowing what other terminals are observing.

4 Preliminary results

A possible application for the presented cognitive-based system is supporting a human operator in performing monitoring tasks (e.g. to block an intruder, to manage or avoid a panic situation). The proposed architecture is divided into two levels to take into account the two different interactions performed by the system:

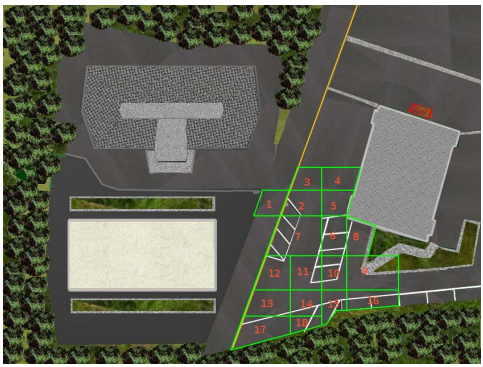

Figure 3: Environment map.

1) interaction with a cooperative operator (e.g. a guardian); 2) interaction with the environment through the operator. The former level is useful to model the relationships between the operator and the system in order to enable a proactive interaction between these two players. The latter model intends to describe how the system can modify the external state by the operator and actuators. Exploiting these two models, the proposed approach aims at learning the interactions in which the two entities are involved and at constructing a correspondent probabilistic representation by which supporting the decision phase through the possibility of predicting future events through acquired experience.

In order to verify the effectiveness of the proposed architecture for the fusion of information coming from video and radio sensors a set of simulation have been carried out. In particular, an outdoor scenario (i.e. a parking lot in the university campus – see Figure 3) monitored with a network of smart cameras and a set of cooperative cognitive radio sensor is considered. The considered area is, then, divided into zones (or cells) and each of them is associated to a label. In this way the space can be described as a graph, where the nodes are the zones of the maps and the branches are associated to a weight depending on the distance between adjacent zones. Besides, using this subdivision, the contextual representation of the target position is the membership to a zone. With this kind of representation messages can be interpreted as the indication to go from a zone to another. In this environment the task of the system is twofold. Firstly, it has to identify illegal access to a restricted area and to detect forbidden and harmful radio transmissions. Secondly, it has to support or drive the operator who performs actions in the environment. For instance, the system has to be able to detect an intruder in a restricted area who wants to perform jamming interference to already existing communications. In the considered applications it is supposed that the intruder can perform jamming actions with Wife [19] and/or Bluetooth [20] communication standards. To detect this kind of signals the system is equipped with a set of cooperative cognitive radio sensors which take as input an evaluation of the position of the intruder and of the cooperative radio sensors obtained by the network of smart cameras. In our example we consider that the evaluation of the required positions provided by

the network of smart cameras are in the range of $\pm$ 1 meter with respect to its actual value. In order to detect the signal transmitted by the intruder the approach proposed in [21] is used. Such an approach is based on distributed detection theory and it exploits the cooperation among the cognitive radio sensor and the network of smart cameras since it needs to know the position of the radio sensors. In Table 1 the classification rate, that is the probability of correctly detect the presence of the intruder's transmissions and related communication standard used, is shown for two and three cooperative cognitive radio sensors. It is possible to remark that the classification rate increase as the number of cooperative sensors increase. When a forbidden radio transmission is detected, assuming that it is possible to distinguish detected targets between guard(s) (e.g. by identifying him by the MAC/IP address of his mobile) and intruder(s), the system has to support the operator in the environment to perform the proper action (e.g. reach the intruder). The Autobiographical Memory, after being trained with a set of pre-defined rules, allows the system to predict intruder's behavior in the simulated environment and to guide the guard anticipating his movement. In Figure 4 an example is presented where the intruder, represented with a yellow circle, is starting from zone 17 and guard, represented with a purple circle, is in zone 2. Intruder's movement from cell 17 to cell 18 suggests to the system a proper reaction that is represented by operator's movement from cell 2 to cell 7. Now, there are some possibilities for the intruder, being able to return to cell 17 or to move towards cell 15 (as a rule we have established that it's not possible for the intruder to choose a movement towards a cell which would minimize his distance with respect to the guardian - see cell 14). After the training phase, probabilities shown in Figure 4 have been obtained showing that the most likely behaviour for the unauthorise subject is trying to escape reaching zone 15. Therefore, according to acquired information, the system is able to predict intruder's behaviour and to guide the operator suggesting as the most likely movement cell 11 which allow the guard to minimize his distance from the intruder and so to improve the possibility of catching him. Therefore, from the simulated approach it is possible to extract significant information collected in the autobiographical memory and to develop a promising application that is able to interpret behaviours and interactions within the subjects. This "embodied" knowledge is used to react to dysfunctional activities as an harmful radio transmission and to understand the behaviour of an intruder in order to allow an operator to face an incoming threat.

5 Conclusions and future work

Resuming, the proposed Cognitive surveillance approach introduces a general framework based on the integration of heterogeneous sensing devices as distributed cognitive radio sensors and a network of smart cameras aiming at building an environment able to interact with its components and with the served users with high level of intelligence. This can lead to develop and provide personal services able to make the users to feel helped and protected by the environment they interact with. The main goal of such systems can be oriented to maintain the security, the safety

Table 1: Classification rate.

	W	B	WB	N
W	59.3%	5.1%	35.6%	0.0%
B	0.6%	73.3%	0.0%	26.1%
WB	32.6%	10.0%	57.4%	0.1%
N	0.0%	0.7%	0.0%	99.3%

(a) 2 cooperative cognitive radio sensors

	W	B	WB	N
W	65.0%	0.0%	35.0%	0.0%
B	0.0%	80.0%	0.0%	20.0%
WB	25.0%	0.0%	75.0%	0.0%
N	0.0%	1.1%	0.0%	98.9%

(b) 3 cooperative cognitive radio sensors

Figure 4: Example of simulated guard movement according to behaviour prediction.

and the comfort of the users in the physical and virtual space they live. According to this paradigm, the proposed approach will provide resources to increase:

- Perceptive capabilities of current systems through the exploitation of smart components both in terms of innovative physical sensors and innovative support to smart detection of events (e.g. modelling of semantic knowledge which allows both a semantic graphical way to represent a particular event domain, efficient recognition algorithms and a probabilistic events interpretation);
- Operators decision capabilities through a fitting representation of links between environment conditions and possible threats with the aim of maximizing security level.

Finally, future steps will concern the scalability of the system simulator and tests on real situations. In particular, the presence of different radio sources, both potentially dangerous or not, and the capability of guiding two or more operators in their surveillance tasks will be explored.

References

[1] Brown, G., Carlyle, M., Salmern, J. & Wood, K., Defending critical infrastructures. *INTERFACES*, **36(6)**, pp. 530–544, 2006.

[2] Luiijf, E.A.M. & Klaver, M.H.A., Protecting a nations critical infrastructure: The first steps. *in 2004 IEEE International Conference on Systems, Man and Cybernetics*, 2004.
[3] Brown, G., Carlyle, M., Salmern, J. & Wood, K., Analyzing the vulnerability of critical infrastructure to attack , and planning defenses. *in INFORMS Tutorials in Operations Research*, 2005.
[4] Hennin, S., Germana, G. & Garcia, L., Integrated perimeter security system. *in 2007 IEEE Conference on Technologies for Homeland Security*, 2007.
[5] Reiter, M. & Rohatgi, P., Homeland security. *IEEE Internet Computing*, **8(6)**, pp. 16–17, 2004.
[6] Lipton, A.J., Heartwell, C.H., Haering, N. & Madden, D., Automated video protection, monitoring & detection. *IEEE Aerospace and Electronic Systems Magazine*, **18(5)**, pp. 3–18, 2003.
[7] Marcenaro, L., Oberti, F., Foresti, G.L. & Regazzoni, C.S., Distributed architectures and logical-task decomposition in multimedia surveillance systems. *Proceedings of the IEEE*, **89(10)**, pp. 1419–1440, 2001.
[8] Hampapur, A., Brown, L., Connell, J., Ekin, A., Lu, M., Merkl, H., Pankanti, S., Senior, A. & Tian, Y., Multi-scale tracking for smart video surveillance. *IEEE Signal Processing Magazine*, **22(2)**, pp. 38–51, 2005.
[9] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. & Cayirci, E., A survey on sensor networks. *IEEE Communications Magazine*, **40(8)**, pp. 102–114, 2002.
[10] Culler, D., Estrin, D. & Srivastava, M., Guest editors introduction: Overview of sensor networks. *Computer*, **37(8)**, pp. 41–49, 2004.
[11] Prati, A., Vezzani, R., Benini, L., Farella, E. & Zappi, P., An integrated multimodal sensor network for video surveillance. *Proc. of ACM international workshop on Video surveillance & sensor networks*, 2005.
[12] Aghajan, H. & Cavallaro, A., *Multi-Camera Networks: Concepts and Applications*. Elsevier, 2008.
[13] Vernon, D., Metta, G. & Sandini, G., A survey of artificial cognitive systems: Implications for the autonomous development of mental capabilities in computational agents. *IEEE Transactions on Evolutionary Computation*, **11(2)**, pp. 151–180, 2007.
[14] Anderson, M.L., Embodied cognition: A field guide. *Artificial Intelligence*, **149(1)**, pp. 91 – 130, 2003.
[15] Damasio, A., *The Feeling of What Happens-Body, Emotion and the Making of Consciousness*. Harvest Books, 2000.
[16] Dore, A., Pinasco, M. & Regazzoni, C.S., A bio-inspired learning approach for the classification of risk zones in a smart space. *Online Learning for Classification Workshop*, Minneapolis, MN, USA, 2007.
[17] Marchesotti, L., Piva, S. & Regazzoni, C., Structured context-analysis techniques in biologically inspired ambient-intelligence systems. *IEEE Transactions on Systems, Man and Cybernetics, Part A*, **35(1)**, pp. 106–120, 2005.
[18] Haykin, S., Cognitive radio: brain-empowered wireless communications. *IEEE J Sel Area Comm*, **23(2)**, pp. 201–220, 2005.

[19] IEEE 802.11-1999, *IEEE standard for local and metropolitan Area Network Part 11: Wireless LAN MAC and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band*, 1999.
[20] Bluetooth SIG Inc., *Specification of the Bluetooth System*, 2003.
[21] Gandetto, M. & Regazzoni, C.S., Spectrum sensing: a distributed approach for cognitive terminals. *IEEE J Sel Area Comm*, **25(3)**, pp. 546–557, 2007.