International Journal of Approximate Reasoning 50 (2009) 666–679

Contents lists available at ScienceDirect

International Journal of Approximate Reasoning

journal homepage: www.elsevier.com/locate/ijar

Credal networks for military identification problems ☆

Alessandro Antonucci [a], Ralph Brühlmann [b], Alberto Piatti [a,*], Marco Zaffalon [a]

[a] IDSIA, Galleria 2, CH-6928 Manno (Lugano), Switzerland
[b] Armasuisse (W + T), Feuerwerkerstrasse 39, CH-3600 Thun, Switzerland

ARTICLE INFO

Article history:
Received 14 January 2008
Received in revised form 22 January 2009
Accepted 29 January 2009
Available online 10 February 2009

Keywords:
Credal networks
Information fusion
Sensor management
Tracking systems

ABSTRACT

Credal networks are imprecise probabilistic graphical models generalizing Bayesian networks to convex sets of probability mass functions. This makes credal networks particularly suited to model expert knowledge under very general conditions, including states of qualitative and incomplete knowledge. In this paper, we present a credal network for risk evaluation in case of intrusion of civil aircrafts into a restricted flight area. The different factors relevant for this evaluation, together with an independence structure over them, are initially identified. These factors are observed by sensors, whose reliabilities can be affected by variable external factors, and even by the behaviour of the intruder. A model of these observation processes, and the necessary fusion scheme for the information returned by the sensors measuring the same factor, are both completely embedded into the structure of the credal network. A pool of experts, facilitated in their task by specific techniques to convert qualitative judgements into imprecise probabilistic assessments, has made possible the quantification of the network. We show the capabilities of the proposed model by means of some preliminary tests referred to simulated scenarios. Overall, we can regard this application as a useful tool to support military experts in their decision, but also as a quite general imprecise-probability paradigm for information fusion.

1. Introduction

In the recent times, the establishment of a restricted or prohibited flight area around important potential targets surveyed by the armed forces has become usual practice, also in neutral states like Switzerland, because of the potential danger of terror threats coming from the sky. A prohibited flight area is an airspace of definite dimensions within which the flight of aircrafts is prohibited. A restricted flight area is an airspace of definite dimensions within which the flight of aircrafts is restricted in accordance with certain specified conditions [17].

Once a restricted flight area is established for the protection of a single strategic object, all the aircrafts flying in this region without the required permissions are considered *intruders*. The restricted flight area can be imagined as divided in two concentric regions: an external area, devoted to the identification of the intruder, where the intruder is observed by many sensors of the civil and military air traffic control and by the interceptors, and an internal area, which is a small region containing the object to protect and the military units, where fire is eventually released if the intruder is presumed to have bad aims.

Clearly, not all the intruders have the same intentions: there are intruders with bad aims, called *renegades*, intruders with provocative aims, erroneous intruders, and even aircrafts that are incurring an emergency situation. Since only renegades

☆ This research was supported by Armasuisse, and partially by the Swiss NSF Grants Nos. 200020-116674/1 and 200020-121785/1.
* Corresponding author. Tel.: +41 586666661; fax: +41 586666670.
E-mail addresses: alessandro@idsia.ch (A. Antonucci), ralph.bruehlmann@ar.admin.ch (R. Brühlmann), alberto.piatti@idsia.ch (A. Piatti), zaffalon@idsia.ch (M. Zaffalon).

0888-613X/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ijar.2009.01.005

represent a danger for the protected object, the recognition of the intruder's aim plays a crucial role in the following decision. This is the identification problem we address in this paper.

The problem is complex for many reasons: (i) the risk evaluation usually relies on qualitative expert judgements; (ii) it requires the fusion of information coming from different sensors, and this information can be incomplete or partially contradictory; (iii) different sensors can have different levels of reliability, and the reliability of each sensor can be affected by exogenous factors, as geographical and meteorological conditions, and also by the behaviour of the intruder. A short review of the problem and some details about these difficulties are reported in Section 2.

In this paper, we propose *credal networks* [7] (Section 3) as a mathematical paradigm for the modeling of military identification problems. Credal networks are imprecise probabilistic graphical models representing expert knowledge by means of sets of probability mass functions associated to the nodes of a directed acyclic graph. These models are particularly suited for modeling and doing inference with qualitative, incomplete, and also conflicting information. All these features appear particularly important for the military problem under consideration.

More specifically, we have developed a credal network that evaluates the level of risk associated to an intrusion. This is achieved by a number of sequential steps: determination of the factors relevant for the risk evaluation and identification of a dependency structure between them (Section 4.1); quantification of this qualitative structure by imprecise probabilistic assessments (Section 5.1); determination of a qualitative model of the observation process associated to each sensor, together with the necessary *fusion scheme* of the information collected by the different sensors (Section 4.2); quantification of this model by probability intervals (Section 5.2). An analysis of the main features of our imprecise-probability approach to information fusion is indeed reported in Section 6.

The credal network is finally employed to evaluate the level of risk, which is simply the probability of the risk factor conditional on the information collected by the sensors in the considered scenario. A description of the procedure used to update the network, together with the results of some simulations, is reported in Section 7.

Summarizing, we can regard this model as a practical tool to support military experts in their decisions for this particular problem.[1] But, at the same time, our credal network can be regarded as a prototypical modeling framework for general identification problems requiring information fusion.

2. Military aspects

This section focuses on the main military aspects of the identification problem addressed by this paper. Let us first report the four possible values of the RISK FACTOR[2] by which we model the possible intentions of the intruder.

(i) `Renegade`. The intruder intends to use his aircraft as a weapon to damage the strategic target defended by the restricted flight area.[3]
(ii) `Agent provocateur`. The aim is to provoke or demonstrate. The intruder knows exactly what he is doing and does not want to die, therefore he is expected to react positively to radio communication at a certain moment.
(iii) `Erroneous`. The intruder is entering the restricted flight area because of an error in the flight path due to bad preparation of the flight or insufficient training level.
(iv) `Damaged`. This is an intruder without bad aims that is incurring an emergency situation due to a technical problem. The pilot does not necessarily knows what he is doing because of a possible situation of panic. A damaged intruder can react negatively to radio communications, as their instruments could be switched off because of electrical failures. A proper identification of damaged intruders is very important because they can be easily confused with renegades.

In order to decide which one among these four categories reflects the real aim of the intruder an appropriate identification architecture should be set up. Fig. 1 displays the structure typically employed in Switzerland. When a restricted flight area is set up for the protection of an important object, the Air Defence Direction Center (ADDC) is in charge of the identification of possible intruders. The ADDC collects the information provided by three main sources: (i) the sensors of the civil Air Traffic Control (ATC), (ii) the sensors of the military ATC, (iii) the interceptors of the Swiss Air Force devoted to Air Police missions. Once this evidential information has been collected, the ADDC performs the identification of the aim of the intruder.

The civil ATC sensors are based on a collaborative communication between the ATC and the intruder. In fact, the detection of the intruder by the ATC is possible only if the intruder is equipped and operates with a *transponder*. Transponders are electronic devices that, if interrogated by the civil ATC radar, emit a signal enabling a three-dimensional localization. Radars based on this principle are called Secondary Surveillance Radars (SSRs). Transponders emit also an identification code. We consider the identification code *Mode 3/A*, which, in certain cases, does not allow the exact identification of the intruder

[1] The support we provide is represented by the probabilistic information about the actual level of risk associated to an intrusion. Decisions about possible interventions can be based on this information, but are still taken by military experts. A model of such decision process, to be embedded into the network structure, could be explored (e.g., by considering the ideas in [1] and their development in [10]), but is beyond the scope of this paper.

[2] The following typographical convention is used: the variables considered in our probabilistic model are written in SMALL CAPITALS and their possible states in `typewriter`.

[3] There are also some subcategories of terrorists (e.g., poison sprayers), which will be considered only in a future work.