Ontology for Complex Mission Scenarios in Forensic Computing

José Helano Matos Nogueira\(^{(1)}\) and Wamberto W. P. Vasconcelos\(^{(2)}\)

\(^{(1)}\) Brazilian Federal Police, helano@apcf.org.br
\(^{(2)}\) University of Aberdeen, w.w.vasconcelos@abdn.ac.uk

Abstract—Complex mission scenarios are those in which information changes continuously and quickly or scenarios having large quantities of expensive resources, a large number of norms and rules, or a large number of personnel, for instance crimes in cyberspace, computer forensics, or computer and digital investigation. Organisations participating in such scenarios may have components in different geographic locations: some in the field and others in the office. Enabling coordination between these components in highly unstable environments is a challenging task. Our aim is to investigate the use of ontology with computational agents to support complex mission scenarios in Forensic Computing. This paper presents a logic- and set-based model to represent scenarios in the context of a formal organisation. In addition, an outstanding ontology was implemented that describes typical mission activities, their relationships, required resources, and constraints. This ontology is used to map a mission to an organisation. We also present a realistic ontology scheme in forensic computing for the Brazilian Federal Police and a case study in which agents from a formal organisation were deployed in complex mission scenarios. This ontology can be easily extended to other police or military forces, and is an efficient tool for managing people and resources.

Index Terms—artificial intelligence, complex mission scenarios, forensic computing, international scientific exchange, ontology.

1. Introduction

Our aim is to investigate the use of ontology with computational agents to support complex mission scenarios in Forensic Computing. An ontology is a model of a real domain that is represented in some declarative formalism. In this way, an ontology associates the names of entities in the universe of discourse (e.g., classes, relations, functions, agents, or other objects) with human-readable text describing what the names mean, and formal axioms that constrain the interpretation and well-formed use of these terms. Formally, an ontology is the statement of a logical theory. We intend to present a logic- and set-based model representing the knowledge aspects...
of a formal organisation. Additionally, an outstanding ontology will describe typical mission activities, their relationships, required resources, and constraints. This ontology can be used to map a mission to organisations such as police or military forces.

In this context a formal organisation can be understood as the planned, coordinated, and purposeful action of agents (human beings or computer programmes) to construct or to achieve tangible or intangible objectives. The general approach is to study existing organisations and fully describe the organisational structure before implementation. Thus, we analyse an organisation as an entity centred in a structural perspective. In this sense, the organisation is a permanent arrangement of physical (static structure) and virtual (dynamic structure) elements. These elements and their actions are defined by agents, abilities, roles, goals, resources, legal and administrative norms, competencies, missions, and complex events so that a certain task may be fulfilled through a system of coordinated division of labour by multi-agent units. Following this, we present fragments of a realistic ontology scheme in forensic computing for the Brazilian Federal Police, and a case study in which agents from a formal organisation are deployed in complex mission scenarios.

Complex mission scenarios are those in which information changes continuously and quickly or scenarios using large quantities of expensive resources, a large number of norms and rules, or a large number of personnel. Examples of complex scenarios include investigations of crimes in cyberspace (e.g., sexual exploitation of children, financial fraud, cyberterrorism, or criminal release of information), computer forensics (e.g., live analysis, botnet detection and prevention, or intrusion monitoring and prevention), and computer and digital investigation, in other words events requiring management of multiple abilities or devices. Organisations participating in such scenarios may have components in different geographic locations: some in the field and others in the office. Enabling coordination between these components in highly unstable environments is a challenging task.

This work seeks to explain the problem of managing complex mission scenarios in forensic computing using artificial intelligence-based ontology.

2. Previous Work in this Area

The missions faced by large organisations are highly complex:
- Large number of personnel;
- Large quantities of expensive resources;
- Large number of norms and rules;
- Significant quantities of rapidly-changing information.

Several studies have appeared describing the use of artificial intelligence techniques in mission scenarios [9, 24, 25, 29, 30, 32, 50]. A good example of this important research field is the International Technology Alliance (ITA) project [20, 21]. The main goal of the ITA project is to retrieve and disseminate information relevant to specific missions within a required resource-frame to maximize the utility of the resource. Maximizing utility encompasses giving priority to more important missions, balancing the quality of information with the energy costs of gathering the data, and storing and disseminating information in a manner promoting effective use:
- Developing mission representations that can be used to determine the data required for a mission;
- Development of available mission scenarios, including those used in police training;
- Modelling, through ontology, the sensors and sources required by a mission.

It is necessary to consider missions as an integral feature of an organisation. In this way, organisations can be seen as societies of agents [1, 6, 8]. Actions and decisions are not the simple outcome of a single, orderly activity: they emerge...
from the ecology of the information process. Hence, the relationship between organisations, missions, and environments becomes a subject of practical study. This relationship was clarified in several previous studies concerning the structure of formal organisations:

Choo [5] developed an understanding of how an organisation may manage its information processes more effectively in order to learn and adapt. His view of information management is broad, encompassing information processes, information resources, and information technologies.

Tarapanoff et al [45] dealt with competitive intelligence and scenarios in formal organisations. They included a methodological proposal for a case study.

Vasconcellos et al [48] present the Model of Organisational Change using Agents (MOCHA) as a means of formally specifying, checking, and simulating organisations and their changes using agents. They define the structure of the organisation without making any assumptions about the internal characteristics of the agents who will populate it. They adopt a normative view of organisations, and capture a notion of social influence through relationships between roles.

Dignum et al [10] discuss how and why organisations change. They identify and classify situations for change and explore how these changes can be made dynamically. In systems where the organisational structure is defined in terms of roles that agents enact, the system is required to adapt as agents move in and out of those roles.

Ferber et al [11] adopt a purely organisational approach in the AGR (Agent, Group, Role) model. Agents are active, communicating entities that enact roles with groups. Groups are sets of agents sharing some common characteristic; they are contexts for patterns of activities and are used to partition organisations and define organisational structure. Roles are abstract representations of functional positions that agents may hold in a group and have associated interaction protocols.

Sichman and Demazeau [44] present the core notions of a social reasoning mechanism, based on dependence theory. This model enables an agent to reason about others, in particular to calculate his dependence relations and dependence situations in formal organisations.

3. Formal Definitions

It is important to prove that the proposed formal model is scientifically valid and realistic. Therefore, we intend to present a logic- and set-based model representing the knowledge aspects of a formal organisation performing as defined below.

Def. 1. Organisation

An organisation O is a pair of static and dynamic structures, explained below.

\[ O = (S, D) \]

where:

- \( S \) represents the static structure;
- \( D \) represents the dynamic structure.

Examples:

- \( O = \text{Interpol} \);
- \( O = \text{Brazilian Federal Police} \);
- \( O = \text{US Army} \).

Def 2. Static Structure

A static structure is a set \( S = \{U_1, U_2, \ldots, U_n\} \), where each \( U_i \), \( 1 \leq i \leq n \), is a unit (def. 3).

Def. 3 Unit

A unit is a physical structure that is complete by it.

\[ U = \langle id, C, N, Rls, Rs \rangle \]

where:

- \( id \) is the name of the unit;
C is a non-empty set of deontic formulae (permissions) representing the competencies of the unit;

N is a non-empty set of deontic logic formulae (permissions, obligations and prohibitions) representing norms the unit must conform to;

Rls is a non-empty set of roles;

Rs is a possibly empty set of resources.

Examples:

\[ S_1 = \{ U_{\text{Directorate}}(\text{General}), U_{\text{Directorate}}(\text{Technical-Scientific}), U_{\text{Directorate}}(\text{Intelligence Police}), U_{\text{Directorate}}(\text{Organized Crime Combat}), U_{\text{Directorate}}(\text{Executive}), U_{\text{Directorate}}(\text{Administration and Logistics}), U_{\text{Council}}(\text{Ethical and Discipline}), U_{\text{Council}}(\text{High Police}), U_{\text{Assistance}}(\text{Legal}), U_{\text{Assistance}}(\text{Technical}), U_{\text{Assistance}}(\text{Internal Control}), U_{\text{Assistance}}(\text{International Relationship}), U_{\text{Institute}}(\text{Criminalistics}), U_{\text{Institute}}(\text{Identification}), U_{\text{Academy}}(\text{Police}), U_{\text{Division}}(\text{Forensic Science}), U_{\text{Sector}}(\text{Drug Abuse Combat}), \ldots, U_{\text{Service}}(\text{Expertise in Computer Crime}) \}. \]

This new representational paradigm of a formal hierarchy can be easily modified to represent other formal organisations. For instance, a structure fragment, \( S_2 \), of the operational units for US Army is represented in a hierarchy according to figure 2.

\[ S_2 = \{ U_{\text{Operational}}(\text{Field Army}), U_{\text{Operational}}(\text{Corps}), U_{\text{Operational}}(\text{Divisions}), U_{\text{Operational}}(\text{Brigades}), U_{\text{Operational}}(\text{Battalions}), U_{\text{Operational}}(\text{Companies}), U_{\text{Operational}}(\text{Platoons}) \}. \]

A structure, \( S_1 \), represents one more complete and extended vision of units for Brazilian Federal Police based on figure 1:

\[ S_1 = \{ U_{\text{Directorate}}(\text{General}), U_{\text{Directorate}}(\text{Technical-Scientific}), U_{\text{Directorate}}(\text{Intelligence Police}), U_{\text{Directorate}}(\text{Organized Crime Combat}), U_{\text{Directorate}}(\text{Executive}), U_{\text{Directorate}}(\text{Administration and Logistics}), U_{\text{Council}}(\text{Ethical and Discipline}), U_{\text{Council}}(\text{High Police}), U_{\text{Assistance}}(\text{Legal}), U_{\text{Assistance}}(\text{Technical}), U_{\text{Assistance}}(\text{Internal Control}), U_{\text{Assistance}}(\text{International Relationship}), U_{\text{Institute}}(\text{Criminalistics}), U_{\text{Institute}}(\text{Identification}), U_{\text{Academy}}(\text{Police}), U_{\text{Division}}(\text{Forensic Science}), U_{\text{Sector}}(\text{Drug Abuse Combat}), \ldots, U_{\text{Service}}(\text{Expertise in Computer Crime}) \}. \]

All functional aspects of the missions are components of the organisational dynamic structure.

\[ D = (M_s) \]

\( M_s \) is the set of missions (def. 8).

Def. 5. Dynamic Structure

All functional aspects of the missions are components of the organisational dynamic structure.

\[ D = (M_s) \]

Def. 6. Action

An action \( A \) is a first-order logic predicate \( p(t_1, \ldots, t_n) \).

The set of all possible actions is \( Acs = \{ A_1, \ldots, A_m \} \), \( 1 \leq i \leq m \).

The actions in Forensic Computing could be related via the following predicate.
Ontology for Complex Mission Scenarios in Forensic Computing

Example:

\[ \text{Def. 7. Resource} \]

A resource, \( t_i \), is a material or immaterial support. Each resource is an asset of a unit and to be used in missions by agents. The set of resources is \( R_s \).

- \( R_s = \{t_1, \ldots, t_n\} \),

where \( t_i, 1 \leq i \leq n \), is the resource from the unit.

The resources supplied for an expert agent in computer crime in a mission could be, for instance:

\[ GTD_i = \tau_i - \tau_i^R \]

where \( \tau_i = t_i \in R_s \).

\[ R_s = \{ \text{functional identity,} \]
\[ \text{mission order,} \]
\[ \text{search authority copy,} \]
\[ \text{forms,} \]
\[ \text{radio communicator,} \]
\[ \text{workstation computer,} \]
\[ \text{duplication media,} \]
\[ \text{connector cable,} \]
\[ \text{expert software,} \]
\[ \text{target documentation,} \]
\[ \text{contact data} \} \]

\[ \text{Def. 8. Mission} \]

A mission is a tuple, \( M = (\text{mid}, D, Acs, R_s) \), where:

- \( \text{mid} \) is the identification of the mission;
- \( D \) is the duration of the mission;
- \( Acs \) is a set of actions associated with the mission;
- \( R_s \) is a set of resources that will be used in a mission.

Missions are the set formed by all missions belongs to a specific organisation. Therefore, the set of all missions is \( M_s \).

\[ M_s = \{ M_1, M_2, \ldots, M_n \} \]

Example:

A complete case study of a typical mission, \( M_1 \), in Forensic Computing:

\[ M_1 = \begin{align*} 
\text{mid} & = \text{mission order(0227 SAR/DP/PC)}, \\
\text{time} & = \text{(1st March 2007, 15 days),} \\
Acs & = \{ \text{preparation(Evidence),} \\
& \text{physical extraction(Evidence, Result1),} \\
& \text{logical extraction(Result1, Result2),} \\
& \text{timeframe analysis(Result2, Report1),} \\
& \text{data hiding analysis (Result2, Report2),} \\
& \text{application and file analysis (Result2, Result3),} \\
& \text{documentation(Report1, Report2, Report3, Outcome)} \} \\
R_s & = \{ \text{functional identity,} \\
& \text{mission order,} \\
& \text{search authority copy,} \\
& \text{forms,} \\
& \text{radio communicator,} \\
& \text{workstation computer,} \\
& \text{duplication media,} \\
& \text{connector cable,} \\
& \text{expert software,} \\
& \text{target documentation,} \\
& \text{contact data} \} \end{align*} \]

\[ \text{Def. 9. Complex Mission Scenarios} \]

This is a new concept created in this work to describe missions undertaken by formal organisations such as police forces. In a practical approach, Complex Mission Scenarios (CMS) are those in which information changes continuously and quickly or scenarios requiring a large quantity of expensive resources, a large number of norms and rules, or a large number of personnel.

In a general way, the resources and roles of the static structure may change or, more likely, the set of agents (and their abilities) associated with a mission changes. CMS scenarios are those in which some critical component changes in a static structure \( (S \rightarrow S') \), in the set of agents \( (AGS \rightarrow AGS') \), or both situations.
where,

\[ S \] is all components of the static structure (def. 2);
\[ \text{Ags} \] is the set of agents (def. 4);
\[ M \] is a mission (def. 8).

### 4. Ontology Case Study

An ontology is the explicit specification of a conceptualization of the real world. The term is borrowed from philosophy, where an ontology is a systematic account of existence. For Artificial Intelligence (AI) systems, what “exists” is that which can be represented [18]. When the knowledge of a domain is represented in a declarative formalism (we create a logic- and set-based model to represent scenarios of a formal organisation), the set of objects that can be represented is called the universe of discourse. This set of objects, and the describable relationships among them, are reflected in the vocabulary with which a knowledge-based program represents knowledge. Thus, in the context of AI, we can describe the ontology of a program by defining a set of representational terms. In such an ontology, definitions associate the names of entities in the universe of discourse (e.g., classes, relations, functions, or other objects) with human-readable text describing what the names mean, and formal axioms that constrain the interpretation and well-formed use of these terms. Formally, an ontology is the statement of a logical theory. Hence, an ontology defines a common vocabulary for researchers who need to share information in a domain. It includes machine-interpretable definitions of basic concepts in the domain and relations among them.

Why would someone want to develop an ontology? Some of the reasons are:

- To make domain assumptions explicit;
- To separate domain knowledge from the operational knowledge;
- To analyse domain knowledge.

We created an ontology to represent the mission scenarios of a real organisation, as an extension of the work described in references 3, 7, and 18. It was necessary to develop an ontology solution using software tools. To achieve this we investigated several ontology computational languages (Chimaera [4], Ontolingua [38], and Protégé [39, 40]). We then created an ontology implementation (figures 3 to 6) for the Brazilian Federal Police using Protégé.

![Fig. 3. Ontology implementation and its components with a mission schema](image)

![Fig. 4. Taxonomy diagram for Brazilian Federal Police using our ontology](image)

A common ontology defines the vocabulary with which queries and assertions are exchanged among agents [50]. Ontological commitments are agreements to use the shared vocabulary in a coherent and consistent manner (figure 5). An ontology scheme is more powerful that any
database. It has propositions, rules, predicates, knowledge, relationships, and constraints. With an ontology it is possible to manage resources, to prove axioms, and to make decisions concerning missions, agents, units, and other components of an organisational structure.

![Ontology with agents in a complex mission scenario](image1.png)

Fig. 5. Ontology with agents in a complex mission scenario

For complex mission scenarios in a police force it is important to answer questions like:

- Which missions are in process?
- Which missions are complex?
- Which agents do possess the ability x?
- Where do I find agents with the abilities x and y?
- Which resources are available for this mission?
- In which unit organisation I can request material resources for mission z?
- Which laws, norms and instructions should be satisfied in mission k?
- Is the level of competence in computer science sufficient to execute mission k?
- Which tasks does agent x need to accomplish to conclude mission k?

We elaborated a complete case study for the Brazilian Federal Police in which our ontology implementation

![Query and answer about missions in our ontology](image2.png)

Fig. 6. Query and answer about missions in our ontology

5. International Scientific Exchange

Due to the complexity of interaction between formalisms and the practical aspects of mission scenarios we have already begun to investigate new formalisms and tools to represent ontologies. Since January 2007 we have examined over 50 references, focusing on the topics of first-order logic, deontic logic, relational algebra, set theory, norms, constraints, and organisational architecture. We have also acquired a vast bibliography in knowledge representation, mainly in specific literature [19, 28, 33, 34, 37]. We have investigated languages and tools to represent our ontology, for instance Protégé [39, 40], Ontolingua [38], and Chimaera [4].

We work with real mission scenarios in the Technical-Scientific Directorate of the Brazilian Federal Police. This has provided several years of experience with missions in the field of combating high-tech crime. Investigating cases by unit and sector we have verified that more than 100 missions (about 40 per cent of the total per year) involve complex or mission-critical scenarios. With this experience we have brought new practical viewpoints to scientific research, aiding the comprehension of real problems and aspects of missions in formal organisations.

This year we sent a Federal Criminal Expert (Brazilian police specialist in computer crime combat) to take part in an international exchange and visit the Department of Computing Science at...
the University of Aberdeen, Scotland, UK, to carry out joint work on the topic “Software Agents to Support Information & Workflow in Police Forces” with Dr. Wamberto Vasconcelos, a member of the ITA project [21]. During this visit several topics were examined concerning agents, norms, deontic logic, the architecture of formal organisations, and other important subjects related to this research. The group also investigated new concepts and visions of knowledge representations, taxonomy hierarchies, ontologies, and mission-critical scenarios. A number of meetings with members of local police organisations, researchers, and professors were organized to discuss these themes. At the end of the visit the work was presented in a seminar entitled “Using Agents to Support Mission-Critical Scenarios” [25]. While the seminar presented encouraging results, this area still requires a great deal of research.

6. Conclusions and Future Tendencies

Our objective was to use ontology to support complex mission scenarios in formal organisations such as police and military forces. This research covered a number of practical and realistic themes. One direction was managing missions using an ontological framework. For the first time, a formal treatment of complex mission scenarios was described [25]. We examined whether complex mission scenarios are only those in which resources and roles may change or a changing set of agents (and their abilities) associated with a mission constitutes complexity. This same approach to mission scenarios may be found in [30, 41, 43].

All of the formalisms were defined mathematically to prove actions by agents, to verify norms and competencies, to check roles, and to carry out the relationships between the organisation and its components. We created a logic- and set-based model to represent aspects of a formal organisation and its components [2, 13, 16, 27], but we intend to study the possibility of using relational algebra to model the relationship between units and agents from an organisation.

In addition, we modelled an ontology that can represent complex mission scenarios in real organisations. It was extended into complete case study of forensic computing based on real cases of the Brazilian Federal Police. In this study, our ontology implementation answered important questions concerning the management of agents and resources. However, it is necessary to improve international cooperation and to enlarge our ontology for new applications in other forces.

Therefore, this is a new research area where applications are developed to manage missions in an efficient way. Major governments (funded jointly by the UK MoD and US DoD), universities (CMU, Columbia, UCLA in US; University of Aberdeen, University of Cambridge, Imperial College in UK), research centres (UK MoD Science Innovation Technology, US Army Research Laboratory), and a considerable number of commercial companies (led by IBM) are facilitating research with ontologies and artificial intelligence techniques for mission scenarios. The Brazilian Federal Police cannot be excluded from this new technology. This work represents the tip of the iceberg in terms of the potential for fighting crime.

References

50 Ontology for Complex Mission Scenarios in Forensic Computing


