Chapter 6

Policy Technologies for Federation and Interoperation of Coalition Networks

Mandis S. Beigi
IBM Research, USA

Seraphin B. Calo
IBM Research, USA

David A. Wood
IBM Research, USA

Petros Zerfos
IBM Research, USA

ABSTRACT

The salient characteristic of a coalition network is that two networks that may have evolved independently are brought together for a common operation. Dynamic communities of interests need to be established among the two networks, and establishing such communities requiring federating the assets and resources available in the disparate networks that make up the coalition. Each coalition partner may have guidelines restricting the operating conditions for working with other partners, and sharing information with the other partners. This chapter presents a life-cycle for policy management in the context of coalition operations which can be used to federate different information assets in a coalition, and allow improved interoperability among different constituents of the network.

INTRODUCTION

A coalition operation entails an ad hoc arrangement between organizations that act together to pursue a common objective. Such a coalition will involve two or more organizations with their own inherent restrictions on how they are allowed to operate. These restrictions are usually stated as a set of policies that govern information security and fusion, and the sharing/dissemination of information. Within a coalition, ad hoc Communities of Interest (Cols) come together, perhaps for only a short time, with different assets such as sensors, sensor platforms,
data fusion elements, and networks, to conduct a task (or set of tasks) with different coalition members taking different roles. The environment is therefore very dynamic, and the policy support for it must provide for the rapid assembly and synthesis of disparate elements while maintaining system security requirements.

A key capability that is typically needed in the context of a coalition operation is to deliver the right information to the right coalition partner, in conformance with the policies of all. The assumption is that each member of the coalition has control of its own network of resources, some of which will also be provided for use by coalition partners.

The flow of information from the organizations’ networks must thus be controlled by a set of coalition policies. All data sent between the coalition members’ networks should be routed through a network of information filtering elements (e.g., secure gateways) that federate data according to the policies of the organizations involved. This network of gateways would enforce policies concerning: what information about each coalition member’s assets will be exchanged with other coalition members; and, who, with what authentication, and under what conditions can access sensor information, and in what form it can be provided. These gateways are thus used to extend current communications frameworks into the tactical coalition environment.

This chapter presents policy technologies for federation and interoperation of coalition networks. To guide the discussion and assist in deriving a set of key requirements for such technologies based on the unique characteristics and functional needs of the target operational environment, a use case scenario is employed that involves a contemporary Peace Support Operation. According to this scenario, UK and US Coalition forces have been deployed into a region to assist the indigenous Government forces. The issues related to information flow interoperability across coalition operations can be divided into three distinct stages: the mission planning stage, the operational planning stage, and the tactical operations stage. Sample policies that address a variety of information requirements such as distribution, information sharing and context awareness as well as various approaches to enforce them in all these phase are elaborated in the context of this scenario.

Over the course of a coalition operations scenario, the policy management lifecycle takes place. It is a multi-staged process that starts with policy authoring and extends to policy deployment and enforcement. In this process, various capabilities and software components are needed to provide the framework that enables policy management. While the same concepts can be applied to manage policies in many different domains, our continuing frame of reference is that of ad hoc sensor networking in support of coalition operations. In such environments, policy management must support the rapid assembly/dynamic control of a network of sensors, platforms, and networks to support multiple concurrent coalition missions.

Two of the key capabilities required at multiple stages in the policy lifecycle are that of policy authoring and analysis.

Policy authoring can be done in a number of ways. Policies can be stated in a natural language and then be converted into policy languages (e.g., SPARCLE, JK2005). There are also alternative approaches that follow a template paradigm, as a natural language interface may not always be required or desirable. When the user completes the specification of a policy, it is saved in a computer-interpretable policy language, e.g., the Simple Policy Language (SPL) from the Distributed Management Task Force (DMTF). Many different types of analysis may be useful in policy management environments. These include conflict checking, which detects whether any two pairs of policies have overlapping condition regions and, at the same time, specify conflicting actions; coverage checking for determining whether policies have been defined for all the intended ranges of input parameters; and dominance checking...