RC24604 (W0807-058) July 9, 2008
Computer Science

IBM Research Report

Intelligence, Surveillance, and Reconnaissance Fusion for Coalition Operations

Tien Pham, Gregory H. Cirincione
U.S. Army Research Laboratory
Adelphi, MD
USA

Dinesh Verma
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
USA

Gavin Pearson
Defence Science & Technology Laboratory
Malvern Technology Centre
Worcestershire, UK

Research Division
Almaden - Austin - Beijing - Cambridge - Haifa - India - T. J. Watson - Tokyo - Zurich

Intelligence, Surveillance, and Reconnaissance Fusion for Coalition Operations[*]

Tien Pham
Gregory H. Cirincione
U.S. Army Research Laboratory
Adelphi MD, U.S.A.
tien.pham1@us.army.mil
greg.cirincione@us.army.mil

Dinesh Verma
IBM T.J. Watson Research Center
Hawthorne NY, U.S.A.
dverma@us.ibm.com

Gavin Pearson
Defence Science & Technology Laboratory
Malvern Technology Centre
Worcestershire, U.K.
agpearson@dstl.gov.uk

Abstract – Coalition operations rely on the fusion, sharing and dissemination of information for a network of disparate Intelligence, Surveillance and Reconnaissance (ISR) assets such as sensors, sensing platforms, human intelligence, data fusion and networking elements. One prominent aspect of this research is the design of policy-aware fusion, that is, fusion that takes policy related to security, resource control, command-and-control, etc. into account. Processes are described for development of fusion algorithms and policy protocols that will enable rapid assembly/dynamic control of ISR assets and associated policy agreements that govern the sharing and dissemination of information to support multiple concurrent coalition missions.

Keywords: Network fusion, policy-based security management, multi-modal fusion, ISR, sensor fabric, coalition operations.

1 Introduction and Motivation

In this paper, we describe research from the International Technology Alliance (ITA) in Network and Information Sciences focusing on information fusion and dissemination for a network of Intelligence, Surveillance and Reconnaissance (ISR) assets. The ITA consists of government, industrial and academic researchers from the United States (US) and the United Kingdom (UK) that jointly conduct collaborative research focused on enhancing distributed, secure, and flexible decision-making to improve networked coalition operations [1].

The overall aim of the research described in this paper is to enable the assembly and dynamic control of ISR sensors, platforms and networks to support multiple concurrent coalition missions. A coalition operation usually entails an *ad hoc* arrangement between two or more organizations that act together to pursue a common objective. Such a coalition will bring together two or more organizations with their own inherent restrictions on how they are allowed to operate which are usually stated as a set of policies (including security and legal policies). Within such an *ad hoc* coalition, *ad hoc* Communities of Interest (CoI's) come together, perhaps for only a short time, with different sensors, sensor platforms, data fusion elements, and networks, to conduct a task (or set of tasks) with different coalition members taking different roles.

This research problem can be formulated as that of maximizing the utility of ISR information given a set of missions and a collection of ISR assets while complying with policy constraints of different members of the coalition. Algorithms are required to create joint ISR plans and deployment configurations to best meet the needs of multiple concurrent and competing missions. A critical element in this formulation is data fusion elements deployed throughout an ISR network, and the constraints placed on their use.

Current research in sensor network fusion tends to focus on the physical sensors and the physical aspects of networking such as bandwidth, power, routing efficiencies and scalability. In this paper we consider sensor network fusion and its relationship with sensor-mission assignment and policy-based security refinement and analysis. The goal of this paper is to show that by jointly considering these three elements the utility of the information from the ISR network can be maximized while provably maintaining the coalition’s security policies.

The remainder of this paper is organized as follows. An overview of dynamic mission focused ISR for coalition operations, approaches to matching coalition missions to available ISR assets, and a motivating example scenario is given in section 2. Section 3 discusses the approaches and requirements for sensor

[*] This research was sponsored by the US Army Research Laboratory and the UK Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the US Army Research Laboratory, the US Government, the UK Ministry of Defence or the UK Government. The US and UK Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon. This paper includes British Crown copyright material.

network fusion in the coalition context. Section 4 describes techniques for policy-based security management, an approach to jointly handle the coalition needs for security and sensor network fusion. Finally, section 5 concludes the paper and presents future work.

2 Dynamic Mission Focused ISR

A primary goal of the collaborative research within the ITA is to develop technology to enable the rapid assembly/dynamic control of a network of ISR sensors, platforms, and networks to support multiple concurrent coalition missions. As such, the coalition needs are:

(1) Rapid assembly and synthesis of disparate ISR elements including assets such as sensors and platforms and policies such as security and sharing/dissemination of information;
(2) Resource efficient management of ISR assets to best meet the needs of concurrent competing missions given available assets and their capabilities, security and C2 policies, and the environment;
(3) Autonomous or semi-autonomous, (re)configuration and (re)tasking of ISR assets to adapt to changing conditions and missions;
(4) Proof that negotiated policies maintain security and interoperability requirements throughout operations.

In a typical coalition operation, an ISR community of interest (CoI) is dynamically formed to conduct joint coalition operations. The ISR CoI will operate across a number of levels of command, and will thus include a number of more focused CoI's within the overall CoI. An ISR CoI can be an ad-hoc team consisting of possibly multiple coalition partners executing multiple concurrent missions/tasks such as border/perimeter reconnaissance and surveillance, camp site surveillance and detection/classification of human activities in concealed/confined spaces. A CoI brings together collections of ISR assets, individualized missions or objectives, and sets of policies that govern information security and fusion and sharing/dissemination of information. The first step is to negotiate and develop joint ISR plans and ISR asset deployment configurations. Given a set of negotiated missions and ISR assets, the objective is to maximize the utility of the information derived from the ISR network while considering resource constraints, asset-to-mission assignments, policy-based security, fusion/filtering and networking conditions. The second step is to deploy the mechanisms, configurations and policies to meet coalition ISR plans that then adapts the ISR network to meet missions and priorities and to respond to events and on-demand management.

An ISR network is an adaptive ad-hoc network of ISR sensors, other sources of data (e.g. humans), platforms, communication systems, etc. that provides actionable Information and Intelligence (I2) to its customers. The sensors may exhibit heterogeneity in a variety of dimensions including passive or active, field of view and regard, range and modality (e.g., biometric, acoustic, radar): similarly there may be significant heterogeneity in the other elements of an ISR network. The elements of an ISR network are illustrated conceptually in figure 1 which focuses on the flow of information around an ISR network in response to a customer's request for information [2].

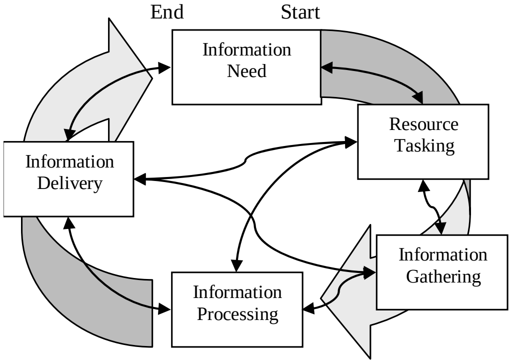

Figure1. Information Flow around the conceptual functional elements of an ISR Network

Next we discuss the ISR assets, which are collection of sensors and sensor systems, sensing platforms, data fusion and networking.

2.1 Sensors/Sensor Systems and Platform

ISR sensors for distributed ground operations can be categorized into low-resolution or "activity" sensors and high-resolution sensors. Activity sensors are typically inexpensive, passive and low-power sensors, and they can provide persistent sensing and broad-area coverage. Typically, they are used to detect the presence of targets such as people and light vehicles and transient events such as explosions and gunfire. Depending on the applications, these sensors can also classify/locate and/or cue other high-resolution sensors. Some of the commonly used activity sensors are acoustic, seismic, magnetic, passive IR (PIR), and chemical/biological. To enhance the probability of detection while reducing the probability of false alarm, many sensor systems take advantage of the orthogonal and complementary information gain from multi-modal fusion of several activity sensors. Figure 2 shows an example of personnel detection via foot steps from a combination of acoustic, seismic and PIR sensors [3].

High-resolution sensors, on the other hand, are generally more expensive, active and high-power sensors. They typically include day-night video and electro-optic (EO) cameras and imagers. If cost and power constraints are not an issue, EO sensors would be the sensors of choice because they can provide the "sensor-to-shoot" capability. In other words, often ISR information becomes actionable when visual confirmation can be established. More recently, small, low-power micro-radar sensors are being use for counting the number of targets and aiding the discrimination between human and non-human targets.

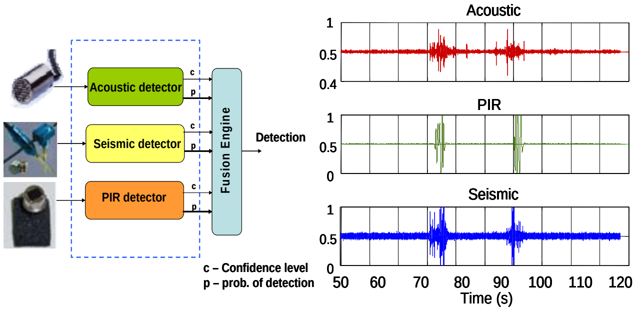

Figure 2. An example of personnel detection via a combination of acoustic, seismic and PIR sensors.

There are a variety of ISR sensor systems currently being used in support of coalition operations. Specifically, for distributed ground operations, Unattended Ground Sensors (UGS) are the most reliable and frequently used ISR systems. The UGS systems are modular and multi-modal, with a combination of activity and high-resolution sensors, and local RF and/or satellite communications to operate in a wide range of weather and terrain conditions. For energy-saving and cost-saving reasons, they are typically configured with only sensor(s) and communication link(s) for the intended missions. UGS systems can be employed/deployed to cover large areas in open terrain (e.g., border region) or in restricted areas such as urban environments. Several scenarios could be envisioned: (i) *Outside looking in* – UGS are employed around a large facility area or small section of a neighborhood city to monitoring suspicious activities; (ii) *Inside looking out* – UGS are employed around a perimeter for base protection to detect/locate incoming intruders or weapon fires; (iii) *Monitoring intersections*: UGS are employed at “choke points” or known paths to specifically provide critical ISR information; and (iv) *Complex terrain* – an ad-hoc network of UGS is distributed in urban terrain, inside/outside structures [4].

As the coalition operations become more dynamic in complex environments, multi-modal sensor systems need to be distributed in space and in time. As such, the mobile ground and aerial sensing platforms are becoming more important. For ISR applications, the mobile ground platforms include military HMMWV’s, unmanned ground vehicles (UGV’s) and small robotic vehicles (e.g., Packbot) [5]; and aerial platforms include unmanned aerial vehicles (UAV’s) and aerostats/balloons [6]. These mobile platforms often provide area coverage gaps or ad-hoc network connectivity; carry expensive high-end/high-resolution sensor payloads; are shared assets supporting multiple missions; are tasks to move to the locations of interest for further ISR information gathering or confirmation; and/or provide communication relays or links for exfiltration of ISR information.

2.2 Security and C2 Policies

When sensor platforms and assets need to be operated in context of coalitions, different policy constraints may need to be incorporated in the operation of the ISR assets. A policy is a constraint limiting the configuration and usage of the ISR assets in the field. The following are the broad categories of policies that are applicable in the context of ISR assets and coalition operations:

- *ISR Asset Characteristics Exchange.* Policies that state what information about sensors and other ISR assets can be exchanged (for the purpose of establishing mission matching, to develop quality of information measures, and to support data fusion) between coalition partners.
- *Local C2.* Policies that delineate the command structure, their roles, their authorizations, and their obligations including who can develop and modify missions, taskings, and policies;
- *Platform Control.* Policies that define whom, with what authentication, and under what conditions platforms (e.g. UAV's, UGV's, vehicles, etc) can be controlled, configured, moved, and re-tasked;
- *Sensor and Sensor System Control.* Policies that define whom, with what authentication, and under what conditions sensors and sensor system can be controlled, configured, moved, re-tasked;
- *Sensor Information Access Control.* Policies that define whom (person, C2 element, data fusion element, etc), with what authentication, under what conditions, and in what form (i.e., raw, processed, fused) sensor information can be accessed;
- *Information Flow Protection.* Policies that define how information flows are to be protected (confidentiality, integrity, etc);
- *Information Dissemination.* Policies that describe the conditions/events under which information must be sent and to whom; the conditions and to whom information can be provided when queried.

Each of these policies can be specified and managed using an architecture with three major components, a *policy manager*, a *policy distributor* and a *policy enforcer*. The policy manager creates, analyzes and transforms the policies to a machine readable format. The policy distributor ensures that the right set of policies have been transferred to the right policy enforcers, and the enforcers are responsible for ensuring compliance with the policies.

Within the ITA program, research is underway to develop a policy management that specifies, analyzes and transforms security policies before they are distributed to the enforcement points. The architecture that is used is shown in figure 3, and consists of policy management through four major stages. In the first stage, policies are specified in constrained natural language specifying the restrictions and access control requirements on the ISR assets. In the second stage, these policies are transformed into an abstract representation. The abstract representation is a computer readable representation, but is not tied into a specific instance of a computer system. In this stage, the policies are analyzed for proper refinement and capturing of the intent represented in the constrained natural language. In the third stage, policies are analyzed for conflicts that may exist between them. If more than one policy set may be in effect, conflicts among the different sets of policies are analyzed and resolved. In the final stage of policy management, policies are transformed to a concrete set that represents the details of the current deployment, and then distributed over to the different set of policy enforcers.

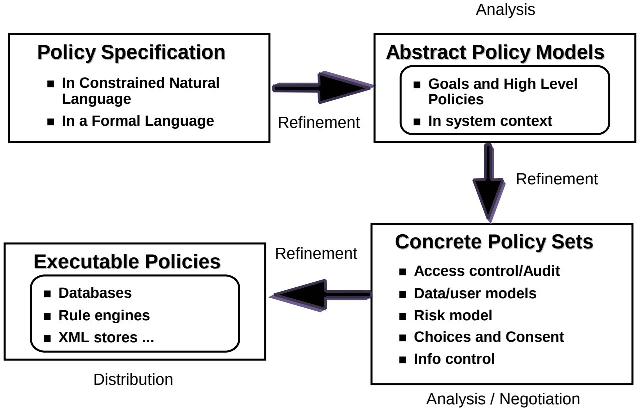

Figure 3. Policy management architecture.

The goal of the different stages of policy management is to ensure that policies are well-formulated and conform to the spirit of coalition operations. Once distributed, the enforcers ensure compliance with the policies as the different ISR assets and information are deployed within the network. A key element of this process is formal analysis to show proof that negotiated policies maintain security and interoperability requirements throughout operations.

2.3 Matching ISR Assets to Missions

The ISR CoI must make effective and efficient use of available ISR assets to gather, process and disseminate actionable I2, while also retaining sufficient resilience to react in a timely manner to unplanned and developing events. This resource tasking and monitoring and management activity must be undertaken during both the planning and execution (i.e., dynamic) phases of a set of missions and tasks, and must mesh with the battle rhythms of the various C2 nodes.

Within the ITA programme, research is underway to develop a (where necessary distributed) method of allocating or apportioning ISR resources (with an initial focus on sensors and their platforms) across a set of missions/tasks in a manner which is aware of the utility of the resources to the missions/tasks, which integrates the sensor catalogue with a sensor ontology and that exploits market-based approaches [2, 7, 8]. The research is also addressing the spatial deployment of sensors, and the dynamic adaptation of the ISR network to meet the needs of a mission/task. The ultimate aim being to address the issues associated with dynamically managing a set of interacting ISR networks which if operated synergistically would be able to better meet the needs of a set of multiple dynamic missions/tasks, but where the individual ISR networks have different local C2's; in other words, how to manage the set of ISR networks as synergistic whole to optimize global utility across a set of dynamic missions where there is competition for ISR resource [2, 7, 8, 9].

2.4 A Motivating Scenario Example

Consider a typical *Peace Support Operation* in which UK and US Coalition forces have been deployed into a region to assist the indigenous Government forces in deterring and/or defeating an active insurgency and reassuring/supporting the local population. In such a case the Coalition (of UK, US and possibly indigenous Government) forces must operate together to (a) protect the forces in the region and (b) dominate the region (to protect and support local population, and deter/defeat the insurgency). This requires the use of ISR networks to provide suitable actionable I2.

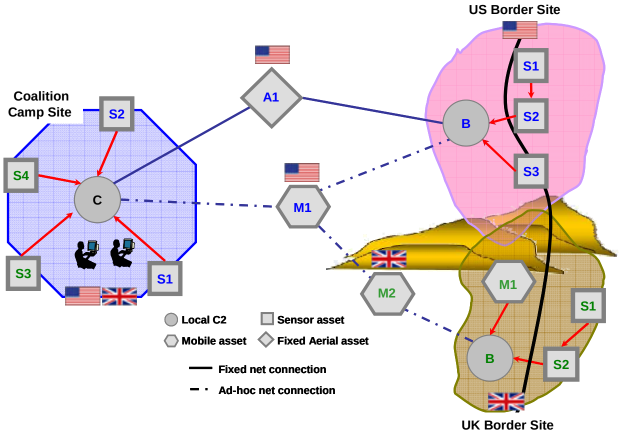

Figure 4. An ISR network scenario with distributed US and UK border surveillance and reconnaissance operations and joint coalition camp site operations.

Simplifying this further consider a scenario with a Coalition base, a border to survey (comprising two relatively open areas and one very rugged area), a main supply route (MSR) and a set of Coalition patrols (both manned ground patrols and UAV's); where the ISR mission is to focus on deterring/defeating the insurgency and protecting own forces. Such a case is illustrated in figure 4, and discussed in more detail below:

- *Base site* – there will be a set of sensors deployed at the base including long range sensors (e.g. an elevated camera), short range sensors mounted at the edge of the base (e.g. CCTV), entry point systems (e.g. biometric & X-ray scanners) and mobile sensors (e.g. troops with binoculars), and near to be base (including UGS and patrols).

- *Border and MSR* – may be covered by a mixture of short range multi-modal UGS (as described above), wide area elevated sensors (e.g., an aerostat with high-resolution EO imagers) and mobile assets (which may be providing observation posts (OP's) and check points, or cued to provide a closer look and/or follow a target of interest).
- *ISR Network* – these sensors are unlikely to be all connected all the time into a single ISR network; this is particularly true when considering mobile assets (which may have low data rate or voice connectivity most of the time, but will only sometimes have high data rate connectivity).

Within this scenario it is entirely possible that there will be a number of issues and concerns (expressed as policies) which impact on the ISR network:

- UK, US and indigenous forces will wish to maintain (at least) a veto on the movement of manned mobile assets outside the base;
- UK forces may be unable due to legal restrictions, arising from different national Rules of Engagement (RoE), to pass precise target locations to indigenous forces, unless target identification criteria matches UK RoE;
- US forces may be unable for security reasons to expose the full capability of a long range imaging system to indigenous forces, but may be able to expose this to UK forces;
- US forces not wish to expose the full capability of biometric sensors, as this may reveal a weakness in their capability which could be exploited.

3 Sensor Network Fusion

The task of fusion of information among the network elements requires two basic functionality – an ability to interconnect dynamically different fusion elements in the network in a flexible manner, and the presence of fusion elements, functional modules that can take as input information from various sources and output a synthesized fused information stream. The ability to interconnect sensors and information sources from distributed coalition forces as shown in figure 4 is provided by the sensor fabric, described in section 3.1. An overview of two local fusion approaches is provided in section 3.2.

3.1 Sensor Fabric

The Sensor Messaging Fabric is an infrastructure that provides a way to interconnect disparate ISR sensors and systems. The fabric uses commercially available messaging software to build a flexible information collection and dissemination infrastructure [10].

A typical messaging system [11, 12] provides the abstractions of multiple virtual message queues that are supported in a distributed manner. Each of the queues is named, such a name being usually referred to as the subject or topic name of the queue. The subject or topic name is the mechanism to link publishers (e.g., data and information produced by the ISR assets) and subscribers (e.g., fusion nodes or end-users) of information. Publishers produce messages on a particular subject or topic name, and subscribers register interest in specific set of subjects. Once an application registers interest on a subject topic, it receives the messages that are created by the publishers of that topic. Information is pushed to subscribing applications as it is generated. Publishers and subscribers can join and leave at any time. The middleware is responsible for routing messages between the publishers and the subscribers.

A typical implementation of the messaging architecture would be through one or more message brokers. End clients or agents register with a message broker, their interest in a topic to receive messages, and also send any messages tagged with the topic name on which it is published, to the message broker. The brokers manage information about the topology of the different publishers and subscribers and route messages between them. Messaging systems provide additional mechanisms to filter, analyze and perform various kinds of access control on the messages that are required for robust operation in an enterprise context.

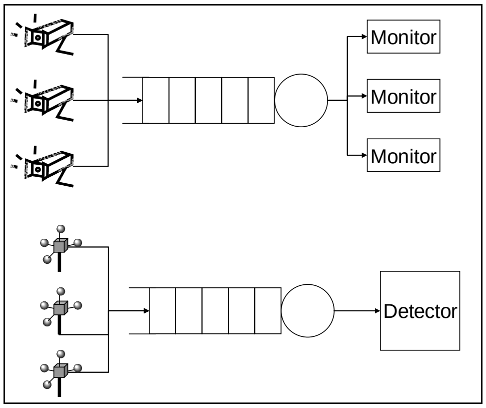

Figure 5. A logical connectivity in Sensor Fabric.

A message queue based sensor fabric connects different sensors using a message queue. Each of the sensors is a publisher on one or more topics and different sensor processing elements receive the information on a published topic. Logically, the sensor fabric allows all ISR assets to be connected to one or more virtual queues (topics). Assuming that the ISR deployment consists of three seismic sensors feeding data to a system detecting for explosions, and three cameras feeding monitors of a guard, the logical interconnection of the data collection, fusion and processing elements are as shown in figure 5. The sensor fabric [13] maps the simple logical abstraction of figure 5 to an internal set of message flows that are routed in an optimal manner within the messaging system from the publishers of the queue to the subscribers of the queue. In a manifestation of the sensor deployment, the physical infrastructure may be the more complex interconnection as shown in figure 6.

Each of the forwarders in figure 6 can act as a fusion element processing the input stream to produce a different stream of information than the one it is receiving. An alternative mode of processing of sensor information would be to have all processing be done at the receiving elements. Either or both of these options can be used depending on the needs of the mission.

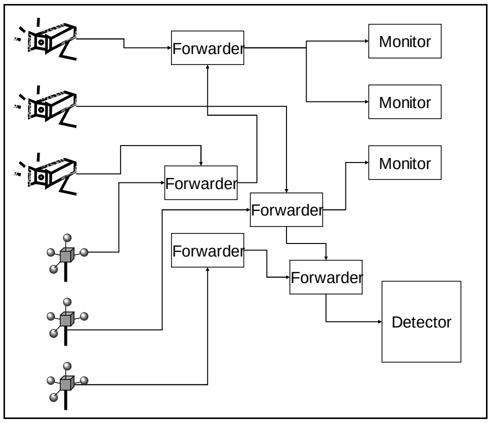

Figure 6. Physical connectivity using Sensor Fabric.

By providing a logical abstraction of topics which hide away the details of physical interconnections and routing among the flows, the message fabric allows for new fusion elements to be connected in an easy manner. When information in the network is being processed by various elements, processing functions can be added dynamically and the task of rerouted information streams in the physical network topology left to the messaging fabric to manage. Thus, the sensor fabric help address the coalition needs (1) and (3) described in section 2.

3.2 Multi-modal and Information Fusion

In this section, we discuss two fusion approaches that can be implemented in conjunction with the sensor fabric for a network of ISR assets. More specifically, at the fusion nodes, the fusion algorithms along with algorithms for security and policy are controlled and supervised by the brokers described above. The first approach is developed at ARL and uses mutual information to fuse multi-modal sensor information. The second approach is developed under the ITA programme and uses ontologies to mediate and augment traditional fusion approaches.

3.2.1 Mutual Information Fusion

Suppose, at the US local C2 site (shown on the top right in figure 4), several sensors (connected to the local C2) of different modalities (e.g., acoustic seismic and PIR as shown in figure 2) have detected an event of interest. The objective at the local C2 is to classify the event via multi-modal fusion. In general, fusion of mixed sensor modalities is not theoretically straightforward because models are not known for the joint statistical dependence between the signals. An information-theoretic approach based on mutual information (MI) is being developed to address this problem [14]. For example, if we were to fuse acoustic and seismic sensor information only for target classification as shown in figure 2, then the MI fusion approach involves two steps: (1) estimate the joint statistics of the acoustic and seismic signals using measured data (training), and (2) fuse the acoustic and seismic data by maximizing a MI criterion. The result of this process is a set of features that combine the acoustic and seismic signals to maximize the information for classification of the targets of interest:

- The MMI features are known to have two properties that provide a sound theoretical justification for their use: Maximizing the MI (MMI) in the features minimizes the bounds on the probability of classification error;
- Features that maximize MI are generalizations of the following well-known and commonly-used feature extraction methods such as Principal Components Analysis (PCA) and Independent Component Analysis (ICA). Furthermore, MMI features reduce to PCA and ICA when the data is described by Gaussian distributions. Consequently, MMI features fully exploit the class distributions in the training data, rather than assuming they follow Gaussian distributions [14].

3.2.2 Semantically-mediated Fusion

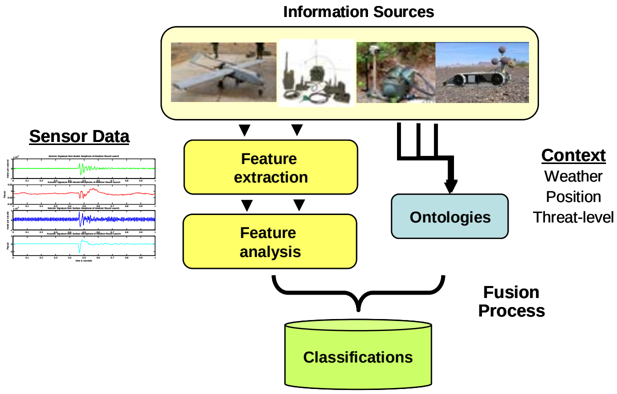

Figure 7: Semantically-mediated data fusion architecture for classification.

Suppose now that at the US local C2, there is other semantic information such as context, trust and/or provenance available. Figure 7 shows an approach in using semantic information to mediate or improve the fusion process at the local C2. The application to fusion is a special case of a general framework to enrich the data using ontology based on semantic information. Ontologies provide semantically precise methods of describing entities or concepts in a domain and the relationships between them; they are used to reason about the data/information within the domain of interest. This approach can augment (without degrading performance) a large class of generic fusion processes.

In an initial application [15], the semantic approach is applied to the problem of classifying military ground vehicles with data from acoustic sensor arrays. In this context, semantic data such as weather, position, threat level, etc., can be incorporated in to the fusion process. In [15], ontological derived features were used to augment the traditional acoustic harmonic features extracted from the power spectra. On average, the classification accuracy improved 5% – 11% depending on the number of semantic data features used for a 5-class ground vehicle classification problem.

4 Policy Based Security Management

In order to enforce and support policy operations for the control and operation of the disparate sensor fusion operations in a coalition context, we need to combine the concept of policy management for coalition operations together with the interconnection of the fusion elements enabled by the sensor messaging fabric.

Policy based security management in coalition operation requires incorporating the impact of policies in 3-stages of a coalition operation as shown in figure 8.

Initially, during the planning of a coalition mission, one needs to take into account the differences in the policies of two different coalition members, and determine any conflicts among them. The conflicts in policies need to be resolved and a set of policies conformant to the requirements of all coalition members needs to be developed.

Subsequently, during the planning of an ISR operation, one needs to determine which coalition member is capable of performing each type of required operation under existing set of policies, identify any conflicts of operations needs with mission policies, and determine the right configuration of ISR assets to support the needs of the missions. This requires a tool that matches assets to operations incorporating policy needs. Finally, as the operation is underway, the different ISR assets need to be configured to support the desired policies. This can be done by enhancing the sensor messaging fabric with policy enforcement capability.

Within ITA, we are developing the basic algorithms required to enable all operation stages of the life-cycle. Towards this goal, our policy validation and analysis research focused on development of conflict detection and validation algorithms for coalition policies. The approach taken for conflict detection is to map each policy into a region in a hyper-space whose axes are defined by the different conditions under which a policy applies. The set of policies defined by each coalition member defines different regions in such a hyper-space. Policies applicable simultaneously are identified by detecting overlaps in the region of the hyper-space, and their actions can be analyzed to detect any conflicts. Negotiations between coalition members can then be used to select the approach that negates the conflict.

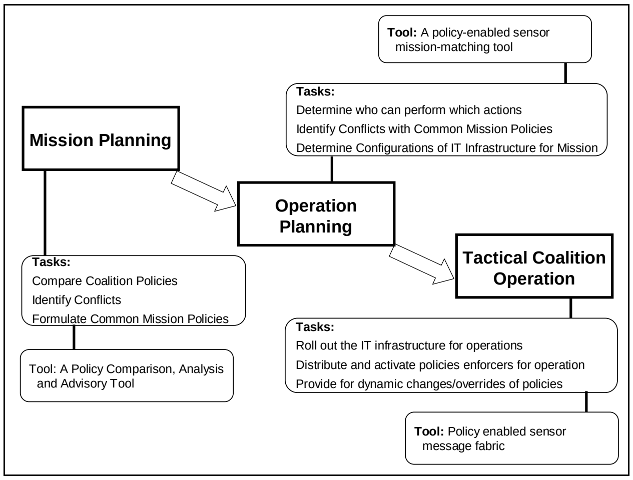
Tool: A policy-enabled sensor mission-matching tool
Tasks:
Determine who can perform which actions
Identify Conflicts with Common Mission Policies
Determine Configurations of IT Infrastructure for Mission
Mission Planning
Operation Planning
Tactical Coalition Operation
Tasks:
Compare Coalition Policies
Identify Conflicts
Formulate Common Mission Policies
Tool: A Policy Comparison, Analysis and Advisory Tool
Tasks:
Roll out the IT infrastructure for operations
Distribute and activate policies enforcers for operation
Provide for dynamic changes/overrides of policies
Tool: Policy enabled sensor message fabric

Figure 8. Impact of policies on coalition operation.

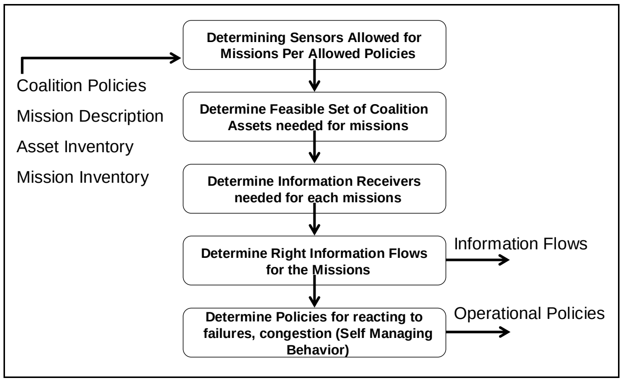
Determining Sensors Allowed for Missions Per Allowed Policies
Coalition Policies
Mission Description
Asset Inventory
Mission Inventory
Determine Feasible Set of Coalition Assets needed for missions
Determine Information Receivers needed for each missions
Determine Right Information Flows for the Missions
Information Flows
Determine Policies for reacting to failures, congestion (Self Managing Behavior)
Operational Policies

Figure 9. Flow chart for policy enhanced mission-asset matching.

In order to augment the sensor mission matching tool with policy considerations, each asset is annotated with the policies available to it for sharing with other coalition members. Thus, the asset-mission matching algorithm is augmented to incorporate policies doing its search. The flow-chart for the process is shown in figure 6. Thus, policy enable mission matching address the coalition need (2) discussed in section 2.

In order to augment the sensor fabric with policy based management, we exploit the flexibility and adaptability of the fabric to insert enforcement points within the information flows carried on by the sensor fabric. As mentioned in section 3.1, the sensor fabric provides the logical concept of topics. The enforcement process for policy integrated sensor fabric consists of defining topics so that the flows across coalition members are always constrained to proceed through policy enforcement points that can validate that the flows conform to the desired policies.

Thus, by enforcing policy mechanisms at each operational life-stage of the ISR operation, a holistic approach to information fusion compliant with mission policies can be developed. Policy management addresses the coalition need (4) discussed in section 2.

5 Conclusion

In this paper, we describe the joint research being performed in the ITA in *Sensor Information Processing and Delivery* and *Security Across a System of Systems* technical areas to develop fusion and policy algorithms and tools to enable the assembly and dynamic control of ISR assets to support multiple concurrent coalition missions. Future work includes further development of the algorithms and tools, simulations via the ARL's *Wireless Emulation Lab*, implementation on a sensor network testbed, and field test demonstration of the technology via a network of disparate UGS systems and sensors on mobile platforms such as UGV's and/or small UAV's.

References

[1] G. Cirincione and J. Gowens, "*The International Technology Alliance In Network And Information Science A U.S.-U.K. Collaborative Venture*", *IEEE Comms. Mag.*, Vol 45, Issue 3, pp. 14-18, March 2007.

[2] G. Pearson and T. Pham, "The Challenge of Sensor Information Processing and Delivery within Network and Information Science research," *SPIE Defense & Security Symposium: Defense Transformation and Net-Centric Systems 2008*, Orlando, FL, March 2008.

[3] R. Damarla and D. Ulford, "Personnel detection using ground sensors," *Proc. of SPIE – Vol. 6562 Unattended Ground, Sea, and Air Sensor Technologies and Applications IX*, May 2007.

[4] N. Srour and T. Pham, "Acoustic UGS for Today's Battlefield," *NATO SET-107 Symposium on Battlefield Acoustic Sensing for ISR Applications*, Amsterdam, the Netherlands, October 2006.

[5] S. Young and M. Scanlon, "Acoustic sensors on small robots for the urban environment," *Proc. of SPIE Vol. 5804 -- Unmanned Ground Vehicle Technology VII*, May 2005.

[6] C. Reiff, T. Pham, et al, "Acoustic Detection from Aerostat," *Proc. of 24th Army Science Conference*, November 2004.

[7] H. Rowaihy, et al, "A Survey of Sensor Selection Schemes in Wireless Sensor Networks," *Proc. of SPIE Vol. 6562 Unattended Ground, Sea, and Air Sensor Technologies and Applications IX*, May 2007.

[8] A. Preece, et al, "Matching sensors to missions using a knowledge-based approach," *SPIE Defense & Security Symposium: Defense Transformation and Net-Centric Systems Conference*, Orlando, FL, March 2008.

[9] G. Pearson, "A vision of network-centric ISTAR and the resulting challenges," *SPIE Defense & Security Symposium: 6562 Unattended Ground, Sea, and Air Sensor Technologies and Applications X*, Orlando, FL, March 2008.

[10] D. Verma, et al, "Policy enabled interconnection of sensor networks," *SPIE Defense & Security Symposium: Defense Transformation and Net-Centric Systems Conference*, Orlando, FL, March 2008.

[11] IBM Software, *WebSphere MQ - Product Overview*, http://www.ibm.com/software/mqseries/.

[12] OSMQ, *Open Source Message Queue*, http://www.osmq.org.

[13] F. Bergamaschi, et al, "A distributed test framework for the validation of experimental algorithms using real and simulated sensors," *1st Annual Conference of the International Technology Alliance*, College Park, MD, September, 2007.

[14] R. Kozick and B. Sadler, "Classification via Information-Theoretic Fusion of Vector-Magnetic and Acoustic Sensor Data," *ICASSP 2007*, Vol. 2, April 2007.

[15] B. Guo, et al, "Approaching Semantically-Mediated Acoustic Data Fusion," *IEEE MILCOM*, Orlando, FL, November 2007.