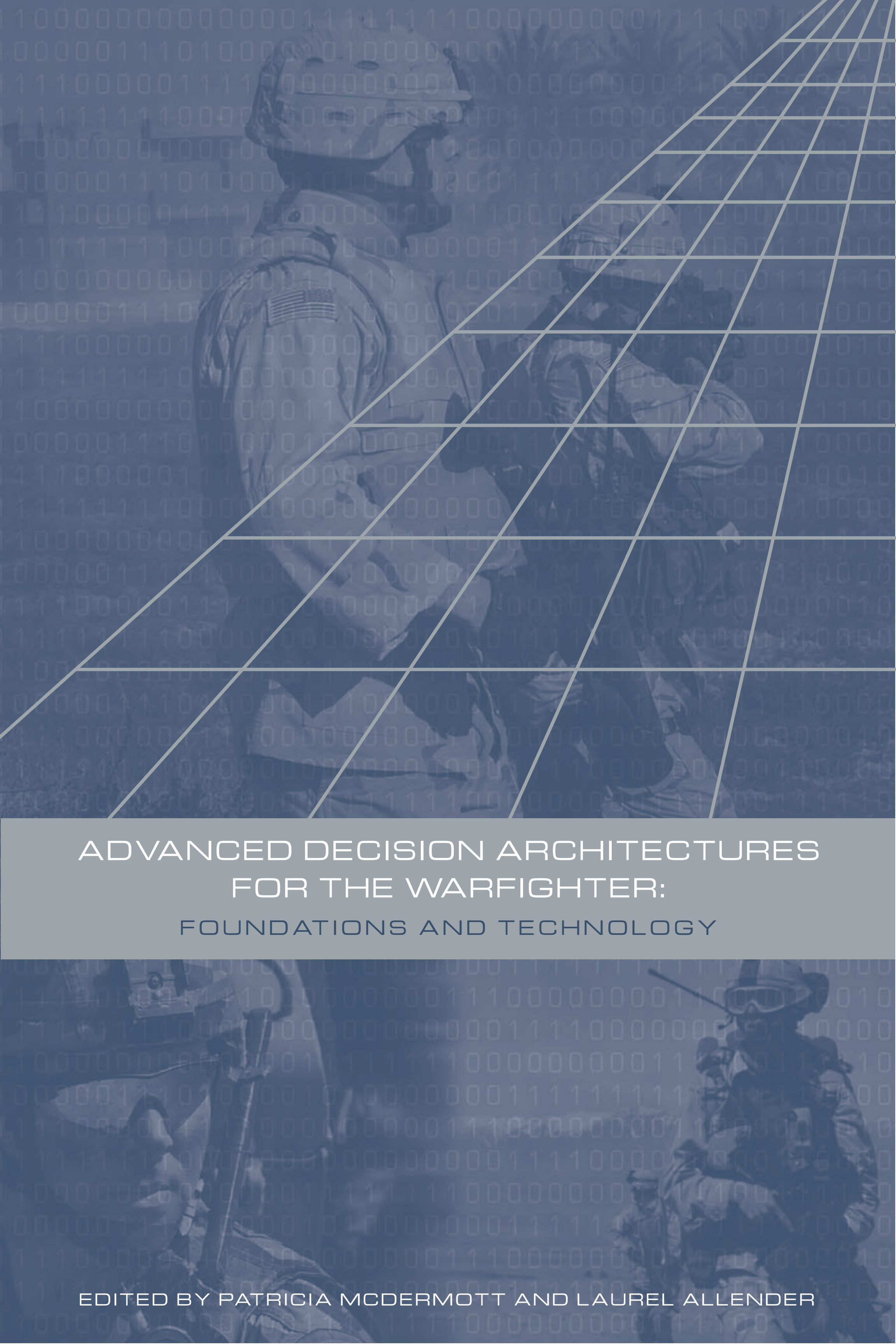


ADVANCED DECISION ARCHITECTURES FOR THE WARFIGHTER:

FOUNDATIONS AND TECHNOLOGY

EDITED BY PATRICIA MCDERMOTT AND LAUREL ALLENDER

ADVANCED DECISION ARCHITECTURES FOR THE WARFIGHTER:

FOUNDATIONS AND TECHNOLOGY

EDITED BY PATRICIA MCDERMOTT
AND LAUREL ALLENDER

This book, produced by the Partners of the Army Research Laboratory Advanced Decision Architectures Collaborative Technology Alliance, also serves as the Final Report for DAAD19-01-2-0009.

SECTION I

COLLECTING, PROCESSING, AND DISTRIBUTING BATTLEFIELD INFORMATION

Chapter 4

REGULATING THE EXCHANGE OF TACTICAL MILITARY INFORMATION USING THE KAOS POLICY SERVICES FRAMEWORK

Larry Bunch, Jeffrey M. Bradshaw, Ph.D.,
Matt Johnson, James Lott,
Paul J. Feltovich, Ph.D., Niranjan Suri, Ph.D.,
Marco Carvalho, Ph.D.
Institute for Human and Machine Cognition, Pensacola, FL

Larry Tokarcik, Robert Winkler, Somiya Metu
Army Research Laboratory, Adelphi, MD

INTRODUCTION

Sharing tactical information among joint forces, coalition partners, and non-government organizations (NGOs) can be critical to successful and safe operations. Unfortunately, the need to share information is sometimes at odds with the sensitivity of battlefield information (McNaugher, 1989; Feltovich, *et al*., 2009). Frequently, the flow of data across heterogeneous channels and among diverse groups must be tightly regulated. This presents significant operational challenges, including successful negotiation of the multi-level, interdependent, and sometimes conflicting agency and interagency aims, governed formally by policy and chains of command, and informally by cultural and organizational norms.

IHMC and ARL are collaborating to develop software systems in which information is passed seamlessly across multiple organizations, networks, and individuals while respecting complex and possibly conflicting sets of policies. In support of this objective, we have created capabilities that allow us to automatically and dynamically identify, in a context-sensitive way, when requisite operational and situational imperatives warrant the automated (or semi-automated) declassification and dissemination of sensitive but perishable combat data. Moreover, we are exploring mechanisms for abstracting and transforming information to enable it to fulfill requirements for sharing, for example, by redacting the content or metadata of messages or by delaying their delivery until a critical situation is over. By providing automated mechanisms to help identify relevant sensitive but perishable data in the Collateral Space that can be released, transformed, or delayed with appropriate levels of human oversight and approval, lives can be saved and time wasted in performing these tedious tasks manually can be significantly reduced or eliminated.

Our approach includes the use of an extensible standards-based policy representation to specify formal policy statements about the tactical domain. The KAoS Policy and Domain Services framework provides a graphical interface for quickly constructing policies in readable English in a point-and-click fashion at run-time. KAoS also provides innovative formal ontology-based policy analysis and deconfliction mechanisms and highly-efficient mechanisms for policy monitoring and enforcement (Uszok, *et al*., 2008). It also includes many powerful features that enhance its usefulness in real battlefield situations (e.g., support for standalone or disconnected operations, spatial and temporal reasoning). We integrate this policy reasoning capability with distributed middleware components capable of enforcing such policies in a MANET (mobile ad-hoc network) environment (Suri, *et al.*, 2003; Carvalho, *et al.*, 2007).

BACKGROUND

Information exchange in a tactical environment is important to the net-centric vision of the Department of Defense (DoD Report, 2001). Warfighters must share information across organizational, national, and spatial boundaries to achieve operational goals. Critical information comes from such disparate sources as manned and unmanned sensors, human intelligence networks, the Internet, and Global Positioning Systems. The tactical environment demands a solution that keeps information protected, is near real-time, can be widely distributed, and accommodates multiple rich information sources. Such mechanisms would allow the movement of certain data in certain situations (e.g., “sensitive but perishable”) across the boundaries between various domains. Ideally, these mechanisms should be automated such that messages, objects, or files can flow securely across the boundary with minimal human intervention. However, it is important that such systems support the appropriate degree of human oversight and approval of the information exchange process.

A prime example of the need to exchange tactical information is the sharing of blue-force tracking data. This information concerns the location, nature, and movement of friendly forces and is precisely the type of perishable tactical data that needs to be shared among multiple cooperating organizations such as US forces, UK forces, NGOs, and local police. Knowing the location of friendly forces and non-combatants is critical to avoiding potential fratricide situations and minimizing civilian causalities. While all of the participating agencies are therefore motivated to share such tracking information, each organization has regulations governing the kinds of data that may be shared with members of the other domains. The information sharing policies required can be complex and require a rich language that can draw upon any aspect of the data as well as the context in which the data is being shared. We have been especially concerned with situations where inflexible, context-insensitive application of policies may endanger lives. For example, when a special operations group unexpectedly moves into close proximity of another group, their normally-undisclosed location may need to be temporarily revealed to reduce the risk of friendly fire.

Current Information Exchange Solutions

One approach to providing information exchange across domains is for each domain to have an independent network that cannot be accessed by members of the other domains. The domains then establish a minimal number of connection points between the networks (US, UK, Police) and share all information across domains through these points where the data can be inspected and filtered. This is DoD's current approach which implements cross-domain information exchange via a security guard or gatekeeper, called a Cross-Domain Solution (CDS) (Crocker, 2007). A CDS confirms that information has been correctly downgraded when traveling from a higher classification domain to a lower one. A CDS applies pre-established rule sets to perform this function, uses standard Internet protocols, and is designed for specific data formats. Examples of security guards are the Radiant Mercury system developed for the Navy and deployed around the world at 150 sites, Oracle Vault selected by INSCOM as part of its filing solution, and the Diamond Matrix CDS developed by the US Air Force. CDS solutions are capable of securely controlling information exchange, but at the cost of prohibiting peer-to-peer data exchange. This gateway approach can lead to circumstances where Soldiers from different domains are collocated, capable of connecting and sharing information peer-to-peer, and authorized to share the information, but forced to send the information through the gateway just to ensure the information sharing is permitted. This can quickly become unacceptable in tactical environments where a connection to the gateway is not always available and timeliness is imperative.

Research Direction

New technology and certification advances are creating opportunities for significant improvement in tactical cross-domain solutions. Certification and accreditation systems based on the old paradigm of “need to know” led to the technology solution of gatekeepers. New certification and accreditation processes are being advanced to reflect the network centric, Web technology based, new paradigm of “need to share.” This shift is toward providing more information sharing capabilities to the edge along with the responsibility for securing the information and complying with the policies and regulations that govern information exchange (Alberts, 2003). This project draws upon recent advances in Agile Computing (Suri *et al.*, 2003, 2008) and cross-layer substrate work (Carvalho, *et al.*, 2007) to realize these capabilities in tactical MANET environments.

Current CDS’s typically use access control techniques that are based on static, a priori assignment of roles, which is limiting in the dynamic battlefield. Current information sharing regulations operating procedures depend on much more contextual information than the users’ credentials, network addresses, and payload. For example, some regulations refer to the perishability of the information (Field Manual 100-8, 1997) which may require temporal reasoning and others depend upon the proximity of units or other spatial relationships. Part of our objective is to show how advances in semantic technologies for reasoning and representation can complement and enhance current solutions for information sharing in complex tactical environments where context-sensitive policy-enabled information sharing is a vital challenge.

INNOVATIONS

The primary innovation of this project is a *policy-governed information exchange software capability* for Warfighters operating in a tactical environment. This software enables policies to be easily developed that will control the abilities for any node in a network to share authorized information with its neighbors. This secure dynamic decentralization of policy specification, deconfliction, analysis, and enforcement is a critical step toward making tactical cross-domain information practical, cost-effective, and flexible enough to meet the needs of new situations as they arise.

A second innovation is a standards-based formal and extensible *policy representation* for describing information sharing conditions and constraints. This representation enables us to provide a rich set of constructs for policy administrators to define the contexts in which information sharing is permitted. These concepts include attributes of the actors involved (e.g., domain, echelon, mission), the information being shared (e.g., type, location, perishability, specific content), and states (e.g., threat level). These semantically-rich policies can permit or forbid information sharing based on any combination of these context attributes (*authorization policies*).

The third innovation is a new form of *information exchange policy* that can require (or waive a requirement for) certain actions to be taken by the policy enforcement mechanism (*obligation policies*). For example, rather than just prohibiting certain information from being exchanged, these obligation policies can require the modification of the information or the process of exchange in a way that makes it permissible. This includes, for example, automated downgrading (e.g., redaction of content, metadata; reduction of resolution of images) of information for certain exchanges. In addition, obligation policies can specify the conditions under which humans must give specific approval for information release. They can also require certain exchanges to be logged and appropriate personnel to be notified in the case of policy violations.

POLICY REPRESENTATION

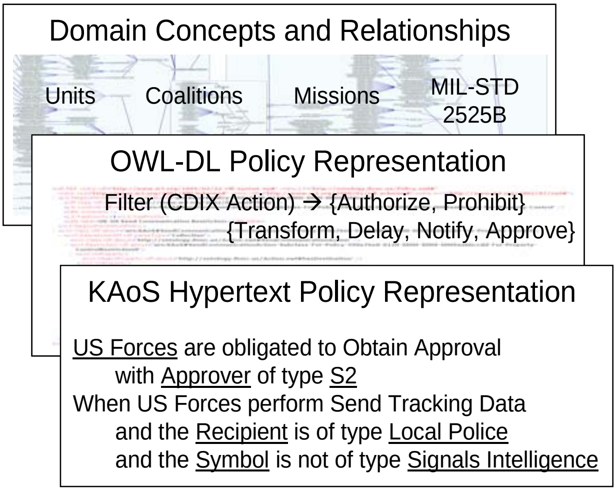
One challenge is to specify information sharing policies in a way that is straightforward for users to understand yet sufficiently expressive to capture the complexity of regulating information exchange in the tactical domain.

The KAoS policy services framework (Uszok, *et al*., 2008) employs the standard W3C OWL (Web Ontology Language) (McGuinness, *et al.*, 2004) to represent policies. OWL is built on top of XML (and RDF), and so it can take advantage of the many third-party tools and applications that have appeared in the last several years. We have found OWL to be a very flexible and efficient approach to policy reasoning and representation, and have overcome a number of technical challenges (e.g., non-monotonic reasoning, increased expressiveness, ease of use, dynamic changes, efficiency, scalability) that have limited the use of OWL in previous applications by researchers (Bradshaw, 2008). KAoS defines the structure of a policy as a mapping from an “Action Class Description” (ACD) describing the context in which the policy applies to an authorization or obligation. The context includes an extensible set of properties describing the Action, Actors, and State in which the policy applies.

KAoS Policy: ACD (Action, Actors, State) →{Authorization, Obligation}

The ACD is defined using *restrictions* in the OWL language to specify the range of values for each property of the Action, Actors, and State that must be satisfied to trigger the policy. To create a vocabulary for tactical information sharing policies, domain-specific concepts were added to the KAoS core ontology. From these concepts, sharing-specific policies can be defined:

Sharing Policy: ACD (Sharing Action, Groups/Roles, Content, State) →
{Authorization, {Transform, Delay, Notify, Approve}}



Domain Concepts and Relationships

Units Coalitions Missions MIL-STD 2525B

OWL-DL Policy Representation

Filter (CDIX Action) → {Authorize, Prohibit}
{Transform, Delay, Notify, Approve}

KAoS Hypertext Policy Representation

US Forces are obligated to Obtain Approval
with Approver of type S2
When US Forces perform Send Tracking Data
and the Recipient is of type Local Police
and the Symbol is not of type Signals Intelligence

Figure 4.1
An ontology of domain-specific concepts are assembled into a formal OWL policy representation which is then interpreted for users by the mediating hypertext policy representation.

Policy analysis and deconfliction algorithms in KAoS can run very efficiently using OWL. Policy decision and enforcement algorithms are even more efficient, due to special OWL “compilation” and caching mechanisms used in the Guard, meaning that most policy decisions can be made in a timeframe that approximates table-lookup. However, the OWL representation is not optimal for human understanding. For this purpose, we developed the KAoS Policy Administration Tool (KPAT) that allows policies to be specified in a restricted form that is closer to natural language.

When the user creates a policy using the generic policy editor in KAoS, he first sees a basic policy statement with a variable number of conditions like the following:

Actor is authorized to perform action with properties

Underlined phrases have a range of possible values defined in the ontology of information sharing concepts and can be replaced with any value from that range. For example, the term "authorized" could be replaced with "not authorized," "required," or "not required." "Actor" could likewise be replaced by a specific individual, group, or role name, and so forth. KPAT uses the familiar hyperlink metaphor enabling one to select these linked phrases to browse the range of possible values drawn directly form the ontology in order to form the desired policy statement as depicted inFigure 4.1. A generic format for an information exchange authorization policy might look something like this:

Actor or Group is authorized to Send Data
when the Recipient has value Actor or Group
and *Context Attribute* has value *Context Value*

The context attributes currently available for governing the action of Send Tracking Data include the context of the sender and receiver including their locations and the domains to which they belong as in the following example:

US Forces are authorized to Send Tracking Data
when the Recipient is of type UK Forces
and the Recipient Location is < 5km from the Sender

We developed an extensive OWL domain model to describe the information content for blue-force tracking including the DoD standard warfighting symbology MIL-STD-2525B (DISA, 2007). This standard defines a hierarchy of approximately 1500 classes of symbols ranging from types of units, installations, and equipment to tactical graphics representing maneuvers, obstacles, and fire support. The top of the hierarchy defines useful high-level abstractions to describe the information such as all Ground Units or Obstacles.

US Forces are authorized to Send Tracking Data
when the Symbol is of type Combat Ground Unit
and the Echelon has value Company or Above

In addition, some policies require an action to be performed as a condition of information sharing. Such obligation policies can require obtaining a particular level of human approval as well as notification to a human analyst or another system. Other obligation actions include transforming, abstracting, or delaying the information to meet the requirements of information sharing constraints:

US Forces are obligated to Obtain Approval
with Approver of type S2
When US Forces perform Send Tracking Data
and the Recipient is of type UK Forces
and the Symbol is not of type Signals Intelligence

Finally, assigning relative priority among policies enables defining abstract ‘default’ policies with layers of (typically more specific) exceptions. For example, a low priority policy may authorize sending all tracking data from US to UK units, but be overridden with a higher priority policy that forbids sharing maneuver tactical graphics. Exception policies of higher priority may similarly be used to override or waive obligations. KAoS also provides an API and user interface for managing policies, a policy repository for storing and querying policies, and a service to distribute policies.

POLICY REASONING

Policy reasoning capabilities are required at each node that exchanges tactical information to determine the applicable policies, assess whether the action is allowed, and provide a list of obliged actions to perform. We rely upon off-the-shelf OWL Description Logic (OWL-DL) reasoning software such as the Java Theorem Prover (Fikes, 2003) and Pellet (Sirin, 2007) to perform the classification of instances into types and subtypes as well as other relationships such as echelons and force structures. This enables the policy system to derive facts from the domain model such as that a Tank is an armored ground vehicle and that a given client is a member of the UK Forces domain.

Specialized reasoning components have been created to support spatial and temporal policy contexts. The spatial reasoning component is able to classify policies based on spatial references such as GPS coordinates, areas, and distances (Uszok, *et al*., 2008). This enables evaluating policy statements such as 'Recipient Location is < 5km from the Sender' or that a blue-force tracking symbol is within an area such as a unit's area of operations.

Additional policy reasoning capabilities include enabling clients to query for the range of possible actions that would be authorized by the current policy set as well as recognizing the potential for policy conflicts at policy creation time. The latter also includes tools to help users resolve such conflicts through policy precedence relationships or further refinement and differentiation of the conflicting contexts.

POLICY ENFORCEMENT

KAoS policy enforcement can be performed in several different ways. In the case of the work under discussions, it is performed by the application middleware that coordinates the peer-to-peer dissemination of data among clients. We use the Agile Computing middleware Dissemination Service (Suri, 2008) to provide and regulate de-centralized information distribution. The Dissemination Service supports store and forward delivery of information by caching data throughout the network, thereby making it tolerant of connection disruptions. Subscriptions to information are organized by hierarchical groups. When information is published in the context of a group, it may also be tagged to identify the type of data (e.g., blue-force tracking, spot reports). Each node in the network running this service processes and communicates subscription requests and published data from neighboring nodes in a distributed, peer-to-peer manner. The dissemination is performed through a combination of push and pull, depending on the number of subscribers, the capacity of the network, and the stability of nodes in the network.

The dissemination middleware has been extended to interact with KAoS policy services to enforce information sharing regulations. The policy decision point implementation, the KAoS guard, provides policy decision capabilities that enable distributed components to get fast policy decisions locally so enforcement can be maintained in environments with unreliable connectivity as shown in Figure 4.2. In this way, information sharing policies can be enforced by the middleware without the cooperation or even the knowledge of the client applications being regulated.

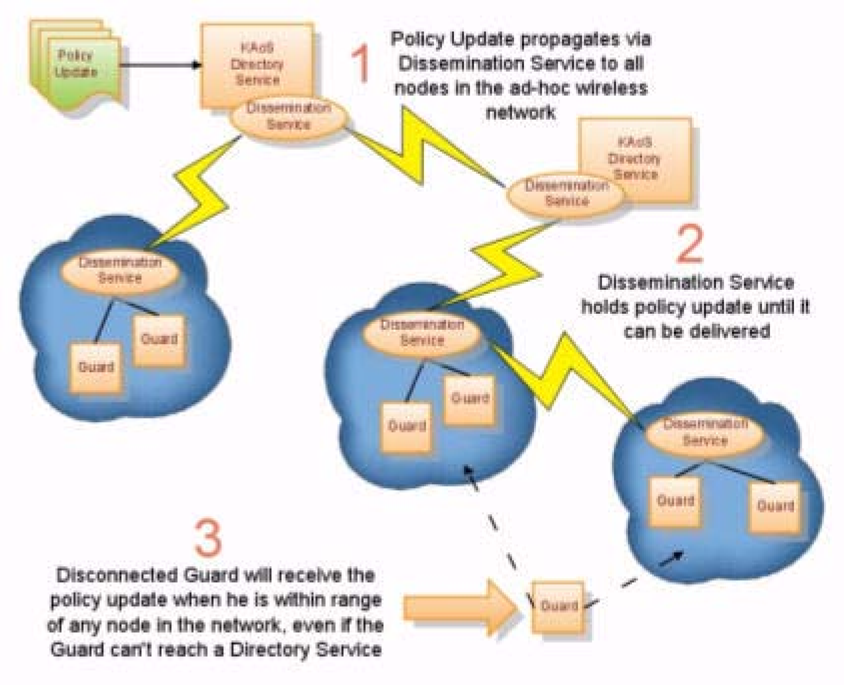

Policy Update
KAoS Directory Service
Dissemination Service
1
Policy Update propagates via Dissemination Service to all nodes in the ad-hoc wireless network
KAoS Directory Service
Dissemination Service
2
Dissemination Service holds policy update until it can be delivered
Dissemination Service
Guard
Guard
Dissemination Service
Guard
Guard
Dissemination Service
Guard
Guard
3
Disconnected Guard will receive the policy update when he is within range of any node in the network, even if the Guard can't reach a Directory Service
Guard

Figure 4.2

Policy changes are distributed through an ad-hoc network by the Dissemination Service to a KAoS guard that serves as the policy decision point for each node.

The Agile Computing middleware components actively inspect the data being exchanged and interact with the KAoS policy services to determine whether an information exchange is authorized and whether any obligations must be fulfilled as depicted in Figure 4.3. In this way, the middleware can allow or block any traffic based on the authorization policies. In the case of obligation policies, the middleware dynamically instantiates components designed to fulfill each of the required actions. The types of obligation actions supported include modifying the message contents, keeping the human in the loop through notification and approval, and affecting the handling of messages by the middleware such as introducing delay.

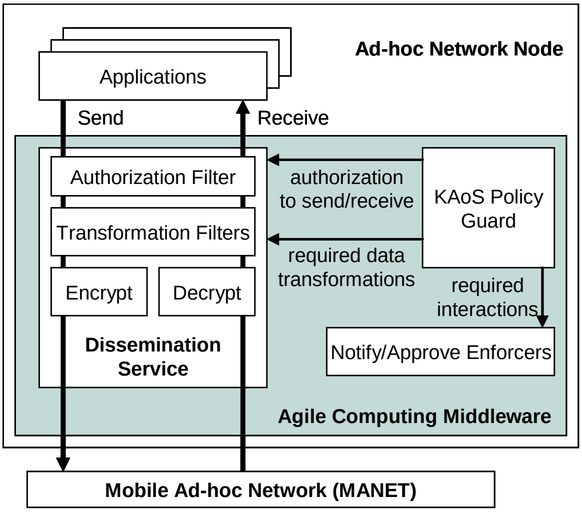


Figure 4.3

Each node in the MANET is equipped with the Agile Computing middleware that manages information access through encryption and enforcing authorization, transformation, and approval policies.

Policy enforcers can automatically redact specified information from messages based on their XML structure and abstract the details concerning unit and other symbol types to a specified level (e.g., showing only that a Unit is a Combat Unit and hiding the details about whether it is Artillery, Infantry, or Armored). An enforcer is also available to transform information including replacing a point-located warfighting symbol with an area tactical graphic such as replacing a unit's identifier and location with a No Fire Zone or replacing observations about enemy forces and targets with Obstacles and Restricted Areas.

Additional enforcers have been developed specifically to maintain human oversight and approval. Policies that oblige approval deploy a component that identifies a user of the specified type or role and interactively prompts the user to allow or deny the interaction.

IMPLICATIONS FOR FUTURE ARMY WORK

Several technical transitions of this work are underway. With training and support from IHMC, our ARL collaborators in Adelphi, MD have adopted the policy language and services innovations from this project for an in-house research effort concerning the automated regulation of information from unattended sensor networks. The framework is being used in specification of *sensor states and activities* as well as domain specific state transition rules which entail information from multiple co-located sensors. The Sensors transmit different types of *alerts*. A single alert or a sequence of alerts within a given time frame can combine to trigger a policy. These policies can be simple or complex depending on the number of alerts in the sequence and the time interval between them. The framework is used to specify, de-conflict, and enforce policies based on these alerts. KAoS is then used to recognize and trigger the highest priority policy which matches any permutation of any combination of alerts from the Sensors. The result is a framework enabling autonomous coordination among sensors to provide smarter alerts.

ARL and IHMC are also extending the policy language and enforcement capabilities to *data gathering* processes such as the harvesting of information from unattended sensors. We believe that policy-governance combined with services to establish *reputation and trust* can enhance data gathering mission effectiveness by managing the limited computation and network resources to help ensure the most important and reliable information is gathered and shared. Tactical military environments are often highly dynamic and consist of fixed and mobile nodes such as unattended ground sensors, robots, dismounted soldiers, ground vehicles, and airborne nodes such as unmanned aerial vehicles. Each of these sources has strengths and weaknesses and the value of the information can vary based on context. These nodes are often interconnected with wireless networks that result in unreliable and bandwidth-constrained links. Due to the large volume of data available with today's technology, it is important to provide automated filtering of data in order to make best use of the limited network resources and also to assist the people processing this data. There are numerous factors that need to be considered when assessing the usability of a given piece of data including the type of sensor, its condition, its history, and its applicability. It is important to make use of this type of knowledge not just at the decision point, but also in the gathering point. Which pieces of data are given priority in the limited network capacity is equivalent to making the decision on what data you will consider and what you will ignore. When providing such a filtering mechanism, it is equally important to allow the users to have some input into that system. The input should come directly, in the form of accessing a sensor's reliability and applicability, and indirectly though the governing policies. In this data gathering context, policy can be used to specify the precedence of the data based on the requestor, objective, and/or the data tag. We support both policy-based prioritization (set by policy administrators at a higher level), and user-requested priority (based on the user's current needs). The two aspects work together to coordinate the flow of data.

The policy capability has also been applied by ARL researchers in Aberdeen, MD to aid Army intelligence analysts in recognizing and navigating the information sharing regulations as they prepare intelligence packages (Mittrick, 2008; Bunch, 2008). This scenario defined a class of Documents with properties such as Classification-Level and Perishability as well as a list of Document Features such as Topography, Routes, Enemy Activity, and so forth. Types of Military Missions such as Peacekeeping and Assault missions were also defined. Each type of Mission is then associated with a list of Document Features that are appropriate for the mission. The ontology was also populated with information about each instance of a document, actor, and mission. For text documents represented in HTML, the RDFa syntax enables embedding the ontology information within the document. For other document types, the metadata is defined externally in an OWL file that contains URL references to each document defined therein. The metadata about each document, the semantic mission-feature-document relationships defined in the ontology, and the policies were all joined together through a query in the SPARQL semantic query language as depicted in Figure 4.4.

Finally, we have worked closely with the US Army Communications Electronics Research, Development and Engineering Center (CERDEC) to identify potential applications for our information sharing policy innovations into two recent projects: Collaborative Battlespace Reasoning and Awareness (COBRA) and Tactical Human Integration of Networked Knowledge (THINK). By combining information with the policies and requirements that govern data sharing, and by applying the underlying semantically-rich representation and reasoning strategies to meaningfully describe and relate information to mission contexts, we believe these technologies can significantly improve the retrieval and sharing of information vital to the Warfighter.

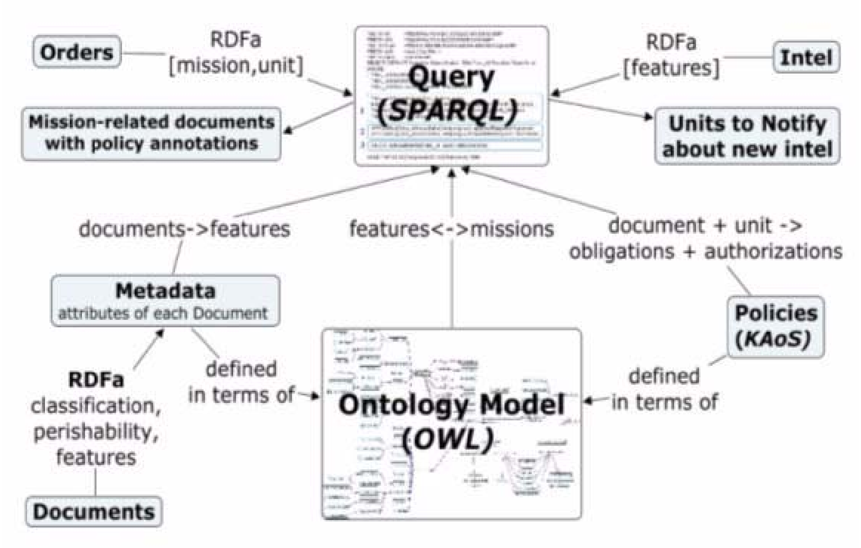

Orders
RDFa [mission,unit]
Query (SPARQL)
RDFa [features]
Intel
Mission-related documents with policy annotations
Units to Notify about new intel
documents->features
features<->missions
document + unit -> obligations + authorizations
Metadata
attributes of each Document
Policies (KAoS)
RDFa
classification, perishability, features
defined in terms of
Ontology Model (OWL)
defined in terms of
Documents

Figure 4.4
ARL and IHMC are combining novel technologies from the semantic web to help analysts identify mission-related intelligence documents as well as recognize and comply with the applicable information sharing policies.

CONCLUSIONS

This research has demonstrated the ability to overcome several barriers to automated information sharing across domains in tactical environments. A key contribution is the extension of an OWL-based policy representation to express meaningful and detailed regulations governing information sharing based on the content as well as the context of the exchange. The KAoS Policy and Domain Services framework provides a graphical interface for defining policies in a natural language format, sound ontology-based reasoning mechanisms for policy analysis and deconfliction, and efficient mechanisms for enforcement (Uszok, *et al*., 2008). It also includes advanced policy services for spatial and temporal reasoning. Finally, we demonstrated an effective approach to automated policy enforcement in a distributed environment by incorporating policy checking and obligation fulfillment capabilities into the application middleware. Through the application of these scientific advances, we have demonstrated the ability to regulate information sharing at the tactical edge.

REFERENCES

Alberts, D.S., Hayes, R.E. 2003. Power to the Edge: Command and Control in the Information Age. Command and Control Research Program.

Bradshaw, J. M. 2008. How to do with OWL what people say you can't. Invited keynote for the 2008 IEEE Workshop on Policies for Distributed Systems and Networks. 2-4 June 2008. Palisades, NY.

Broome, B. D. 2005. Actionable Intelligence for the Warfighter. Invited Talk at the 2005 Netted Sensors Workshop. 24-26 October. McLean, VA. http://www.mitre.org/nettedsensors/2005

Bunch, L., Bradshaw, J.M., Young, C.O. 2008. Policy-Governed Information Exchange in a U.S. Army Operational Scenario. In Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks. 2-4 June 2008. Palisades, NY.

Carvalho, M., Suri, N., Shurbanov, V. & Lloyd, E. 2007. A cross-layer substrate for the battlefield. Pensacola, FL: IHMC Position Paper.

Crocker, M. 2007. Cross-Domain Information Sharing in a Tactical Environment. Crosstalk Journal of Defense Software Engineering. March 2007. http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html

MIL-STD-2525B Common Warfighting Symbology. 2007. Defense Information Systems Agency (DISA).

DoD Report to Congress. 2001. Network Centric Warfare. 27 July 2001. http://www.defenselink.mil/cio-nii/docs/pt2_ncw_main.pdf

Feltovich, P. J., Bradshaw, J. M. & Bunch. 2009. Policy and social barriers to new military information technologies. Pensacola, FL: IHMC Technical Report.

Field Manual 100-8. 1997. U.S. Department of the Army Headquarters.

Fikes, R., Jenkins, J., & Frank, G. JTP: A System Architecture and Component Library for Hybrid Reasoning. Proceedings of the Seventh World Multiconference on Systemics, Cybernetics, and Informatics. Orlando, Florida, USA. July 27 - 30, 2003.

Kean, T.H., Hamilton, L.H., et al. 2004. The 9/11 Commission Report. National Commission on Terrorist Attacks Upon the United States.

D. McGuinness, F. van Harmelen, OWL Web Ontology Language Overview. http://www.w3.org/TR/2004/REC-owl-features-20040210/.

McNaugher, T.L. 1989. New weapons, old politics. Washington, DC: Brookings Institute.

Mittrick, M.R., Richardson, J.T., Kaste, R.C. 2008. A Policy-Driven Information Exchange Network. Army Research Labs Technical Report ARL-MR-704.

Sirin, E., Parsia, B., Cuenca Grau, B., Kalyanpur, A., Katz, Y., Pellet: A practical OWL-DL reasoner. Web Semantics: Science, Services and Agents on the World Wide Web, v.5 n.2, p.51-53, June, 2007.

Suri, Niranjan, Jeffrey M. Bradshaw, Marco Carvalho, Maggie R. Breedy, Thomas B. Cowin, Raul Saavendra, and Shriniwas Kulkarni. 2003. Applying agile computing to support efficient and policy-controlled sensor information feeds in the Army Future Combat Systems environment. Presented at the Annual U.S. Army Collaborative Technology Alliance (CTA) Symposium, April, 2003.

Suri, N., Benincasa, G., Formaggi, S., Winkler, R., Choy, S., Kovach, J., and Tokarcik, L. 2008. DisService: A Peer to Peer Information Dissemination Service for Tactical Environments. In Proceedings of the 2008 Meeting of the Military Sensing Symposia (MSS) Speciality Group on Battlespace Accoustic and Seismic Sensing (BAMS 2008).

Uszok, A., Bradshaw, J., Lott, J. Breedy, M., Bunch, L., Feltovich, P., Johnson, M. and Jung, H. 2008. New Developments in Ontology-Based Policy Management: Increasing the Practicality and Comprehensiveness of KAoS. In Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks. 2-4 June 2008. Palisades, NY.