Enabling information management systems in tactical network environments

Marco Carvalho, Andrzej Uszok, Niranjan Suri, Jeffrey M. Bradshaw, Philip J. Ceccio, et al.

Marco Carvalho, Andrzej Uszok, Niranjan Suri, Jeffrey M. Bradshaw, Philip J. Ceccio, James P. Hanna, Asher Sinclair, "Enabling information management systems in tactical network environments," Proc. SPIE 7350, Defense Transformation and Net-Centric Systems 2009, 73500N (29 April 2009); doi: 10.1117/12.818850

SPIE.

Event: SPIE Defense, Security, and Sensing, 2009, Orlando, Florida, United States

Enabling Information Management Systems in Tactical Network Environments

Marco Carvalho, Andrzej Uszok, Niranjan Suri and Jeffrey M. Bradshaw
Florida Institute for Human and Machine Cognition (IHMC)
40 South Alcaniz St., Pensacola, FL 32502,

Philip J. Ceccio
Northrop Grumman Corporation,
2000 NASA Blvd, Melbourne, FL 32904

James P. Hanna and Asher Sinclair
Air Force Research Laboratory,
525 Brooks Road, Rome, N.Y., 13441

ABSTRACT

Net-Centric Information Management (IM) and sharing in tactical environments promises to revolutionize forward command and control capabilities by providing ubiquitous shared situational awareness to the warfighter. This vision can be realized by leveraging the tactical and Mobile Ad hoc Networks (MANET) which provide the underlying communications infrastructure, but, significant technical challenges remain. Enabling information management in these highly dynamic environments will require multiple support services and protocols which are affected by, and highly dependent on, the underlying capabilities and dynamics of the tactical network infrastructure.

In this paper we investigate, discuss, and evaluate the effects of realistic tactical and mobile communications network environments on mission-critical information management systems. We motivate our discussion by introducing the Advanced Information Management System (AIMS) which is targeted for deployment in tactical sensor systems. We present some operational requirements for AIMS and highlight how critical IM support services such as discovery, transport, federation, and Quality of Service (QoS) management are necessary to meet these requirements.

Our goal is to provide a qualitative analysis of the impact of underlying assumptions of availability and performance of some of the critical services supporting tactical information management. We will also propose and describe a number of technologies and capabilities that have been developed to address these challenges, providing alternative approaches for transport, service discovery, and federation services for tactical networks.

Keywords: Tactical Networks, IMS, Information Management Systems, Federation Services, MANET, discover, simulation, AIMS, Quality of Service.

1. INTRODUCTION

The state-of-the-art MANET technology is still far from being able to fully abstract the demands, constraints and dynamics of tactical environments. The notion of applications and systems that are fully independent of the communications infrastructure is gradually being replaced by network-aware applications that can monitor and adapt to changing network conditions. Those too, are being quickly extended to include application-aware network services, allowing networks and communication systems to autonomously adapt, to the extent possible, to application requirements. The problem is further aggravated in complex and distributed applications such as those envisioned to support tactically deployed Information Management Systems (IMS).

The concept of Information Management Systems was originally conceived by the Air Force Scientific Advisory Board (SAB) at their 1999 Summer Study [0,2]. Entitled the Joint Battlespace Infosphere (JBI), the vision of IMS proposed the seamless integration of information from a wide and diverse variety of sources, as well its aggregation and dissemination

Defense Transformation and Net-Centric Systems 2009, edited by Raja Suresh, Proc. of SPIE Vol. 7350,
73500N · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.818850

in the proper format and granularity to the appropriate consumers. The goal for JBI is: "… provide the warfighter access to the right information in the right format and at the right time."

Critical to this concept in tactical deployments is the ability to share and disseminate information in an efficient and predictable manner. This requires a number of support services and capabilities that greatly rely on the underlying communications infrastructure. When deployed over tactical and mobile network environments, such services are protocols are similarly affected by the dynamics of the communications infrastructure, often leading to a significant degradation, or absolute failure of conventional (enterprise-based) Information Management Systems.

The remainder of this paper will present and discuss the characteristics of tactical communications environments in which net-centric information sharing is envisioned to operate. We will also introduce the Advanced Information Management System (AIMS) and describe how it currently provides information brokering in a tactical airborne environment. Further, we will highlight some of the current deficiencies of the AIMS system and present ongoing research that is intended to address some of these deficiencies. We will also briefly discuss a number of related technologies that have been developed, and are currently being developed, to address the many challenges presented by tactical networks environments. We will provide detailed coverage of the challenges and requirements facing tactical information management as well as the available approaches and strategies that can be leveraged to meet these challenges. Finally, we propose a set of experiments that will enable the measurement of the effectiveness of our system in light of our stated requirements.

2. REQUIREMENTS AND TECHNOGOLOGY CAPABILITIES FOR TACTICAL IMS

Information Management Systems that are lightweight and scalable are necessary to enable shared situational awareness for warfighters in the tactical domain. These systems differ from enterprise solutions due to a number of environmental stressors common to airborne networks. Airborne Networks possess dynamic traits that far exceed those of traditional terrestrial MANET networks. Adaptive IMS must minimize disruption and maintain a reasonable Quality of Service (QoS) in the context of rapidly changing topologies and link quality.

The Advanced Information Management System (AIMS) is a Tactical Information Management System that has been cooperatively developed with Air Force Research Laboratory (AFRL), and industry research partners. At the AIMS core is the AFRL Apollo [1, 2] reference implementation. Authentication, publication, subscription, query, and discovery services are provided by Apollo in the AIMS core. AIMS also serves as an application for reducing risk in development of several critical technologies essential to achieving robust IM capabilities in the tactical domain.

Information node advertisement, discovery, and federation capabilities must support the MANET concepts of spontaneous, self-forming, self-healing networks while maintaining information spaces. This would also include support for roaming ground forces, and transitory users (for example, rapidly moving entities in the battlespace attaching, obtaining services, and detaching as their connectivity to the network changes).

To maintain federated information spaces, federation services must also address occurrences of node entry, handover of information (policy based), and node failovers. Approaches to these issues must include redundancy of information maintained by federates, federation policies, and node connectivity management.

2.1 Message Dissemination Capabilities

An effective message dissemination mechanism is key for tactical information management support. The capability to seamlessly adapt to changes in the underlying communications infrastructure while maintaining IMS-level QoS requirements is critical to support an effective operation of resource allocation mechanism (which often happen is a larger time scale than link-level changes), and to provide reliable state information sharing and control channels for QoS management. Amongst a number of possible solutions to this problem, we will focus on two that have been developed as part of our collaborative research efforts with the Air Force Research Laboratory.

Topology-Aware Adaptive Message Dissemination

The XLayer substrate implements a Message Dissemination capability as one of its core services, available to other services and overlay systems. The Message dissemination service is topology-aware and message type agnostic. The service includes two core capabilities, a) it adapts to IMS-level requirements and underlying resource availability to locally choose a dissemination strategy that best fits the conditions, and b) it seamlessly bridges across the different dissemination strategies for efficient message propagation.

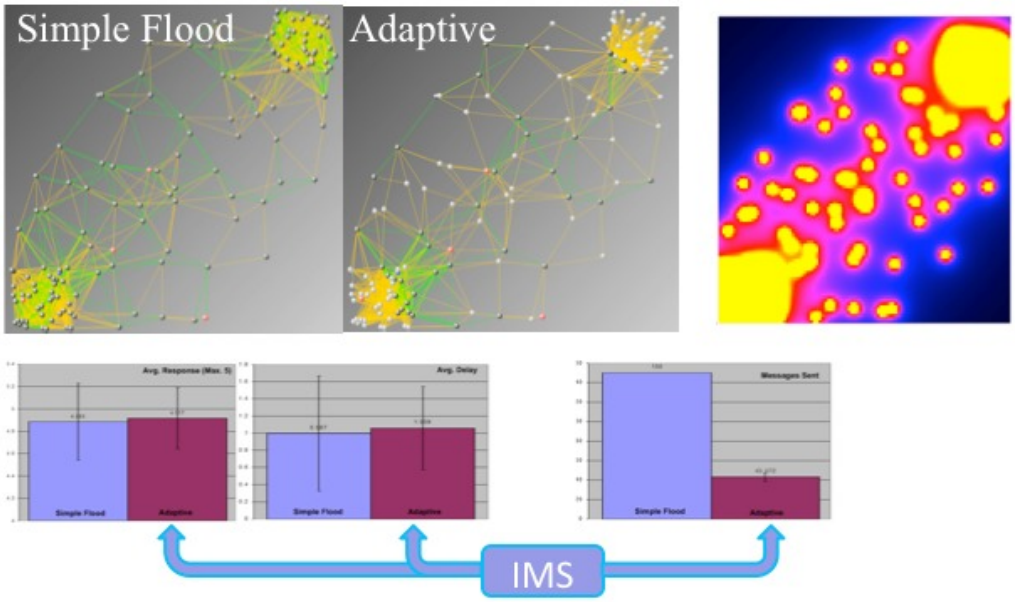

Figure 1. Adaptive Flood Strategies for Information Dissemination

In Figure 1, we show a simple illustration of adaptive dissemination in a mixed-density network topology. In this example and absolute flood is used for comparison. The Message dissemination service locally switches to a more efficient MPR-based flood on high-dense areas of the network. As illustrated in Figure 1, adaptive dissemination significantly reduces the overhead of a full dissemination (more than 60%) maintaining statistically the same levels of coverage and performance. Further reductions in dissemination overhead and be achieved if the IMS chooses to relax the coverage and performance requirements – which is a realistic option in some contexts.

The Agile Computing Dissemination Service

Another core technology developed as part of the Agile Computing Infrastructure, DisService is a peer-to-peer information dissemination system [11]. DisService supports store and forward delivery of data and caches data throughout the network, thereby making it disruption tolerant and improving availability of data. In keeping with the philosophy of agile computing, DisService opportunistically discovers and exploits excess communications and storage capacity in the network to improve the performance of information dissemination.

DisService also supports the notion of hierarchical groups and subscriptions to organize the information being disseminated and to be efficient about delivery of information. Information is published in the context of a group, and may also be tagged to differentiate between multiple types of data (for example, blue-force tracking, sensor data, logistics, or other runtime information).

Each node in the network running DisService operates in a distributed, peer-to-peer manner while processing and communicating the published information and requested subscriptions from neighbouring nodes. Information is disseminated using an efficient combination of push and pull, depending on the number of subscribers, the capacity of the network, and the stability of nodes in the network.

One of the goals of the system is to dynamically adapt to dissemination patterns that are combinations of {one | few | many} nodes to {one | few | many} nodes. Observations of information needs in tactical environments identified three primary modes of dissemination. Situation Awareness (SA) data, such as blue-force tracking information, is one-to-many since it needs to be disseminated to most, if not all, nodes in the network. Directed data, on the other hand, is by nature of interest only to a small subset of nodes. Hence, it is one-to-one or one-to-few. Examples of this type of data include sensor data being transferred to a node for processing or fusion. Finally, the last mode is for on-demand data, which includes large objects such as maps, pictures, videos, and other multimedia objects. Given the limited bandwidth of the network, this type of data should not be delivered until explicitly requested by some node in the network.

2.2 Monitoring and Control Capabilities

One of the key capabilities for the development of tactical applications in general is the visibility and controllability of the underlying communications infrastructure. For enterprise networks, most systems are agnostics of the underlying behavior and constraints of the network. A well-defined layered system provides isolation between the different functionalities of the communication systems and allows for the development of common transport APIs that can be directly used by applications, regardless of the underlying structure of the communications systems.

While the notion of portability and abstraction provided by a layered system is certainly a desirable feature, the approach is generally not applicable to dynamic wireless networks. The fluidity and structure-less nature of the networks, associated with other factors such as interference and resource contingency tends to require the design of systems that are network-aware and can both monitor the relevant state of the network, and influence its behavior to satisfy (to best possible level) system requirements.

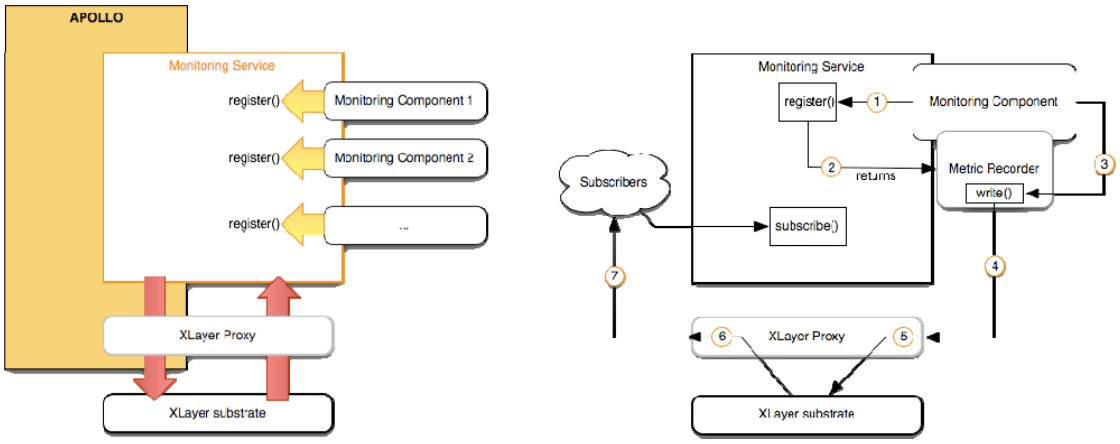

Figure 2. Monitoring Service Capability. Proof-of-Concept integration with the Apollo IMS

As part of our research in QoS-enabled Dissemination infrastructures and Seamless Federated Infospaces we have developed a generic mechanism for system monitoring that enables communication services an overlay systems and middleware to share state information. The monitoring service, as illustrated in Figure 2 provides two core capabilities that are fundamental for tactical environments: a) A common API for metric registration, lookup and subscription from multiple components at the node level, and b) An efficient mechanism for sharing state and monitoring information between nodes, allowing for extensive lookup capabilities of monitoring data.

The monitoring service encapsulates the XLayer internal monitoring capabilities to create a general-purpose blackboard system for metric registration and storage. Each metric is associated with tag that, once assembled with a pre-defined hierarchical structure, creates a unique identified for the metric. For instance, a system component tracking the CPU usation in a node may use the monitoring service to register the metric with a pre-defined 2-byte metric-ID. Before being stored, the metric-ID is combined with a node ID that uniquely identifies the particular metric. When monitoring information is shared between nodes the full key identifies the host and metric that it refers to. The metric identifier (for CPU in this case) is defined in a shared dictionary that includes unique IDs for different types of metrics.

Metrics are created as and stored as short time series, so lookup information includes details about last update, maximum and minimum values, averages, variance and trends. Currently the size of the series is configurable but static through the life of the application – current developments and enhancements to the monitoring component are being made to support adaptive queue lengths, to control the footprint of the service.

The application layer can access the monitoring information either using a polling mechanism, i.e. every time the application needs to know about statistics for particular metrics it simply query the monitoring service, or using a subscription technique. The latter is useful in the case an application needs to adapt its behavior according with predefined conditions (e.g. trigger a particular event in case the local CPU usation increases above some threshold). The API managing the subscription mechanism has been designed for flexibility: it provides the capability of subscribing for being notified every time a metric is updated. Alternatively it enables the application to subscribe for being notified only if a metric

changes violating a pre-established range of values, evaluating either the last value assigned to that metric, the average calculated within a time interval or the average computed using all the available values.

2.3 Service and Platform Discovery for Tactical Information Management Systems

The XLayer communications substrate implements a number of discovery mechanisms implemented on top of its core services for data dissemination and topology monitoring. Different discovery strategies have widely different characteristics and resource requirements. The XLayer substrate supports the online switch between discovery strategies and the co-existence of simultaneous discovery mechanism working on different areas of the networks, seamlessly bridging across the different protocols.

Based on IMS-level requirements and low level topology and load information, different nodes may locally choose (in negotiation with their peers) an appropriate strategy for service discovery. Discovery adaption is different than the data dissemination adaption strategies (item 2.1). While dissemination defines how messages are exchange between nodes to ensure the required covered and reliable dissemination of information, the discovery service defines how registration records are shared and stored across-the network.

For example, one of the discovery protocols implemented in the XLayer is the CDS-based discovery. The algorithm is favored for small world topologies, with dense regions. An efficient approximate algorithm for Connected Dominant Set (CDS) construction [10] is used to create a dynamic backbone that will be used as basis for registration. The properties of a CDS define that every node in the network is either part of the CDS backbone or is directly connected to a CDS node. The property enables the construction of discovery algorithm that shares registration keys through the backbone in a way that specify bounds for the lookup tasks.

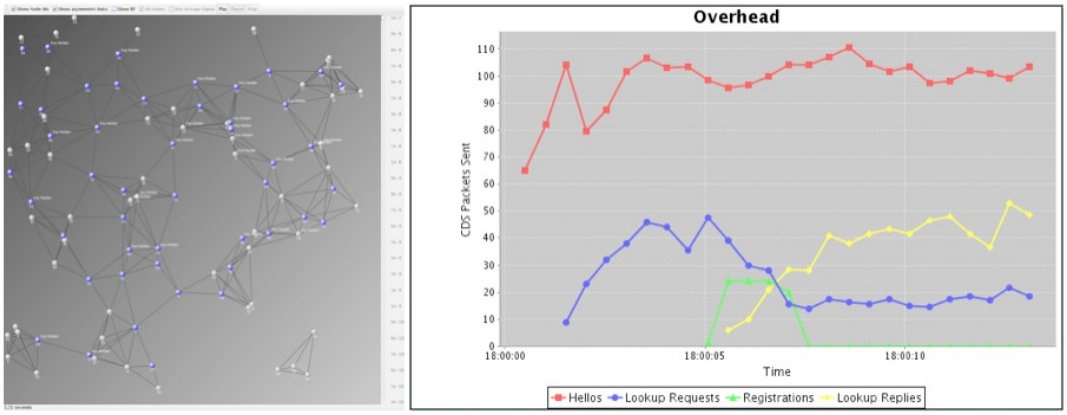

Figure 3. CDS-Based Service Discovery with bound lookup (or registration) hop-distances.

As illustrated in Figure 3, the costs associated with the lookup (estimated by the number of lookup requests) bounded (below 20, in this example) on every time step, while the number of lookup replies increases to approximately the total number of registrations. The initial overhead of the lookup requests is a feature of the search expansion that occurs over the backbone when no records are found. The graph also shows the number of hello messages exchanged by OLSR (also used to maintain the CDS) on each time interval for comparison.

Grouping-based discovery is also supported by the XLayer substrate. The capability is provide by the Grouping Service and allows overlay systems and applications to create and join groups that are used to create a scope for registration and lookup. The Groping Service implements the same API developed for the Agile Computing Group Manager and currently replaces that capability for most of our research projects.

In configured to do so, the XLayer grouping service can automatically construct data dissemination trees based on group registration. The XLayer supports both MOLSR (9) and OLSR MPR-based multicast (BMF). A group defines a search scope, which can overlap or include other scopes. The Grouping Service also implements the Group Manager capabilities for persistent search and for a horizon-based advertisement and lookup (or search) propagation.

Similarly to the CDS-based approach, there is a natural trade off between registration and lookup costs. A broader dissemination of a service registration will make that information readily available in a larger part of the network, and thus more accessible to local searchers. Alternatively, a small horizon for information dissemination can be used to restrict

the proactive availability of a service. The same is true for the horizon metric of the group-based search. Broader searchers will cover a larger horizon and likely retriever a larger set of (possibly 'distant') registrations. From an local node perspective these capabilities can be used in coordination with their resource availability and willingness to provide the service, from a systemic point of view, an IMS may specify policies that will determine (on a group by group basis) the resources involves with service and platform information advertisement versus the lookup-associated costs.

The actual dissemination mechanism used to share information within the group is adaptive and may change deepening on the scale and local density of the network. Based on pre-defined IMS preferences (such as coverage, reliability or performance) the XLayer will favor different protocols for different network conditions and will seamlessly bridge across different protocols possibly running in different parts of the network.

2.4 Transport Capabilities for the Tactical Environment

The Mockets Library provides the transport capability to applications and is a replacement for TCP and UDP sockets. The design and capabilities of Mockets were motivated by observations of problems experienced in tactical network environments, which are typically wireless and ad-hoc with low bandwidth, intermittent connectivity, and variable latency. Mockets addresses specific challenges including the need to operate on a mobile ad-hoc network (where TCP does not perform optimally), provides a mechanism to detect connection loss, allows applications to monitor network performance, provides flexible buffering, and supports policy-based control over application bandwidth usation.

Mockets supports both stream and message-based abstractions. The stream-based abstraction supports exchange of a reliable and sequenced stream of bytes like TCP, which simplifies adapting existing applications that use TCP to use Mockets.

The message-based abstraction provides many enhanced capabilities that are only possible when transmitting individual, self-contained messages as opposed to a continuous stream. These capabilities are:

- Different classes of service – unreliable / unsequenced, reliable / unsequenced, unreliable / sequenced, and reliable / sequenced.
- Tagging of messages to group messages into different categories (for example, for different types of data such as video, voice over IP, and control.
- Prioritization of messages, either individually or by category (based on the tags assigned to messages).
- Replacement of messages – where old and outdated messages can be replaced by newer messages in order to reduce network traffic.

Other key features of Mockets include: a) Application-level implementation of the communications library in order to provide flexibility, ease of distribution, and better integration between the application and the communications layer; b) Transparent mobility of communication endpoints from one host to another in order to support migration of live processes with active network connections; c) Interface to a policy management system in order to allow dynamic, external control over communications resources used by applications; and d) Detailed statistics regarding the connection and data transfer, which allows the application and the middleware to observe the status of a connection and adapt as necessary to observed problems such as connection loss, data accumulation, or significant retransmissions.

Mockets has been integrated into AIMS and was used in a live flight test of a J-STARS aircraft communicating with a ground station via a PRC-117 radio. Performance measurements indicated that Mockets performed 762% better than TCP in the experiment that was conducted. The Mockets library is further described in [4].

2.5 Federation Capability Support

Our federation mechanism supports the interconnection of multiple, independently-managed AIMS information spaces in order to share information. Federation is a key technology to enable cooperation of both joint and coalition forces. We have developed a set of interfaces to facilitate dynamic, runtime discovery and federation of other AIMS infospaces. We have also extended the IHMC KAoS Policy and Domain Services framework [5] to enable semantically-rich policy-based control over the federation and exchange of information. Our approach allows clients to perform publish, subscribe, and query operations across all the federated information spaces in a secure and transparent manner.

The crucial initial capability for tactical Federation is its ability to dynamically discover and opportunistically establish connection with new federates. Fort his purpose, we are using a discovery mechanism that has been implemented using

the XLayer cross-layer substrate [3]. The XLayer substrate also provides a monitoring service that maintains detailed statistics and trends regarding the behavior of the network and the federation. For example, statistics such as CPU load, bandwidth used per connection to each remote federate, and the hit rate for remote predicates.

Statistical information is used by the adaptation mechanism, which automatically and dynamically changes the behavior of the federation to adapt to changing runtime conditions. For instance, one way we handle CPU-overload situations, is to temporarily suspend predicate processing for remote subscriptions. The subscriptions are sorted based on the hit rate of their predicates and successively disabled until the CPU is no longer overloaded. Turning off local evaluation of remote predicates implies that all publications that match the type are sent to the remote federate. Predicates with a high hit rate (i.e., ones that match a large number of published objects) are selected first, since disabling their evaluation increases the bandwidth used by the minimum amount possible. Another adaptation handles a network overload situation in the connection with a remote federate. It temporarily disables remote subscriptions for selected subscriptions. The subscriptions are chosen based on their priorities, which are specified by the remote clients.

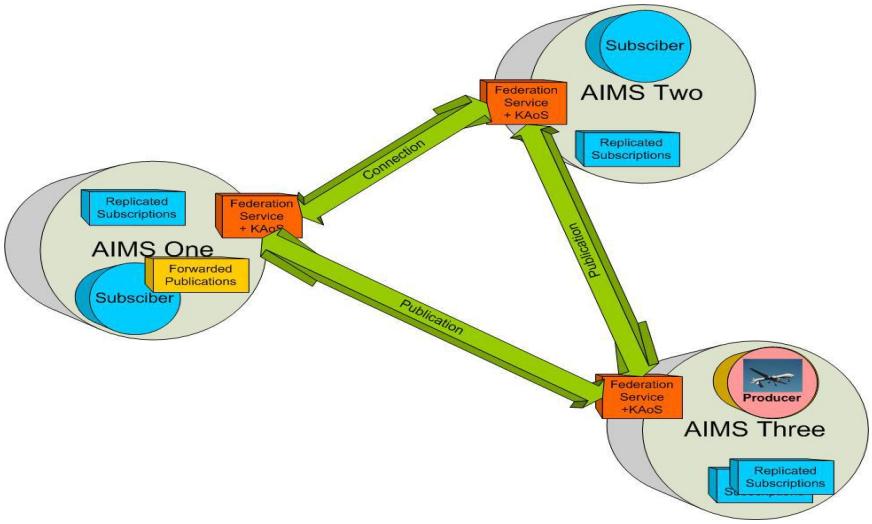

Figure 4. Federation of three AIMS-based infospheres

Connections to remote federates use the Mockets communications library [4]. Mockets replaces TCP sockets and provides transport capabilities for the FCs. Mockets provides significant performance enhancements in wireless tactical environments through specific features such as bandwidth limitation, message replacement, prioritization, and detailed statistics.

The behavior of all the components in the Federation Service is dynamically controllable at runtime via policies. The Federation Service of each federate is integrated with the KAoS Guard software component, which stores policies controlling establishment, lifecycle, information exchange and adaptation of the federations established by this federate. When the new potential federation partner is discovered and the initial connection is established the federate sends its configuration information to its partner federate. Based on this configuration information as well as its own local policies, each federate independently decides:

- Whether to establish a federation with the remote federate,
- What priority to attach to the remote federate,
- Based on the current resource usage for the federation operations and the assigned federate priority, how to estimate the quantity of resources it can devote to server requests from the federate,
- What metadata type subscriptions or queries it would be able to realistically support for a given federate.

During subsequent subscription exchanges, queries, and publication with federates, each operation is analyzed with respect to current policies. These policies may allow or prevent a given operation. They may also modify the operation by changing the subscription or query predicate, or by removing metadata from the published information object being forwarded to the remote federate. They may also enforce or waive obligations (e.g., logging) relevant to certain types of operations. In addition, policies and the agreed adaption matrix control how and when a given adaptation mechanism is activated when the share of resources used by the given federate exceeds the agreed-upon limit.

2.6 Seamless Support for Heterogeneous Tactical Radios and Data Links

Tactical military networks often involve multiple communication systems and data links. A Tactical Information Management System greatly benefits from an underlying communications infrastructure that abstracts the differences and particularities of the different systems, providing a common view of the communications infrastructure.

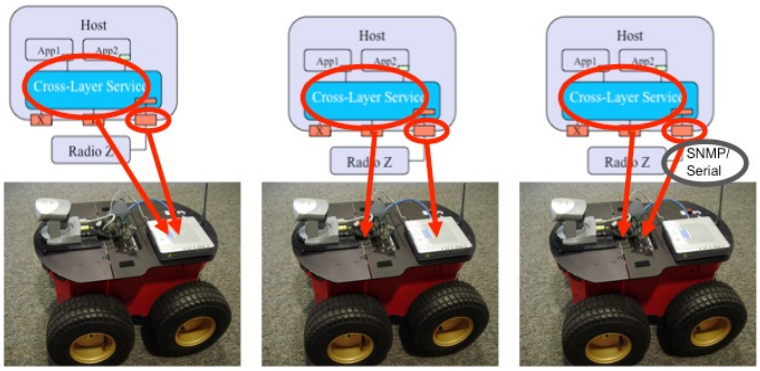

Figure 5. Deployment Strategies for the XLayer Service and Specialized Network Adaptors

The XLayer communications substrate was designed to provide such abstraction to overlay IMS or tactical middleware. The modular architecture enables the instantiation of specialized adaptors for legacy systems and creates a common view of the network across the multiple interfaces. One of the challenges associated with multi-interface support is the fact that different radios expose different kinds of interfaces with widely different APIs and control capabilities. The underlying assumption is that a particular node (i.e. a computational platform or a stand-alone radio system) participates in one more (possibly highly heterogeneous) networks.

The XLayer substrate provides the interface between the Information Management Systems and the underlying communication components. As illustrate in Figure 5, there are three basic deployment strategies for the specialized XLayer adaptor and the main XLayer service.

- The radio adaptor modules and the Xlayer service reside together at the radio system itself. If supported by the radio, this option allows for XLayer service to be executed as part of the radio system, at the same time scale and with local access to all its monitoring and control APIs. In previous research efforts we have adopted this deployment strategy for COTS 802.11 radios with an internal, programmable computing platform.
- The radio adaptor executes as part of the radio system while the XLayer service executes in the base platform. This deployment strategy has also been applied in situations where computational resources in the radio are limited. The adaptor is remotely connected to the XLayer service but the radio is handled as a local interface to the platform.
- The third deployment mode consists on having both the XLayer service and the interface adaptor running at the host and interfacing with the tactical radio through an Ethernet, serial or USB interface. This deployment has been used in demonstrations and experiments to support tactical radio systems such as EPRLS, PSC-5D and serial Microhard (MHX) radios.

When an interface adapter is instantiated, a corresponding object is created at the level of the network manager (an XLayer core service). The network manager handles the each interface differently while maintaining a common view of the communications interface to the overlay IMS. The use of customized adapters for different tactical radios to the overlay data dissemination services.

The Network Manager provides a common interface to other XLayer services for data dissemination (with broadcast, unicast and multicast support). Unless otherwise specified by the applications, broadcast messages sent through the cross-layer API are aggregated and scheduled for distribution with period messages used for instance route maintenance or estate dissemination. As illustrated in Figure 6, redundant information across multiple messages is compressed in a bitmap heading each message in the packet. The goal of message aggregation is to support both the opportunistic dissemination of packets and differential aggregation for different interfaces to better comply with MTU and slot allocation constraints of some tactical radios.

Another benefit of message aggregation is that it greatly reduces the costs of link sensing, used by the XLayer to build link statistics (through periodic beaconing) for radios and interfaces that don't provide a monitoring API. Link sensing is done with a periodic small 4-byte packet sent by each node (Figure 6). Link quality estimation is done at the receiver side and periodic (at a much lower frequency) round trip checks are performed to build two-way link quality estimates. Sensing messages carry a validity time, which allows them to tolerate transmission delays so they are commonly appended to any traffic going across the link. Sensing packets are sent independently only in the absence of other traffic.

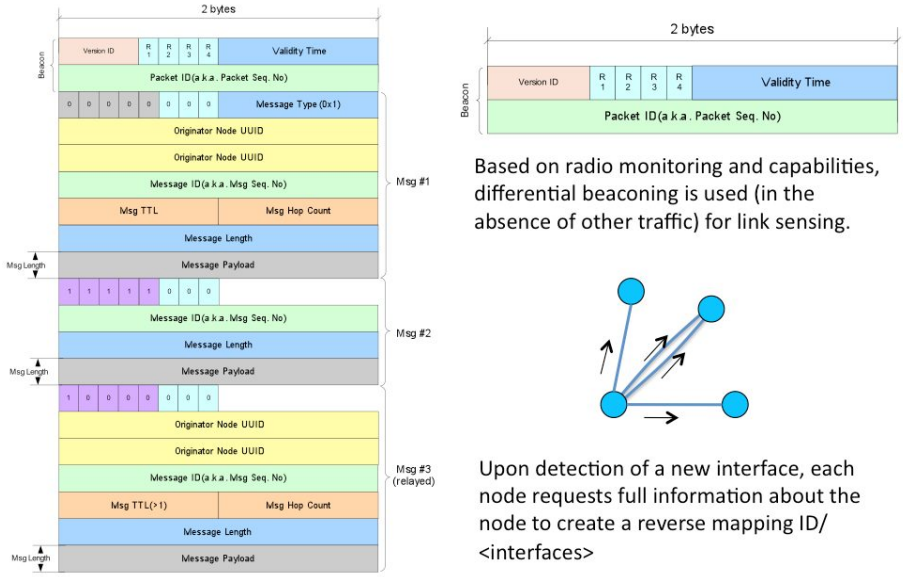

Figure 6. Differential Message Aggregation Strategies for Tactical Interfaces

The integrated message propagation service and sensing capabilities implemented as part of the XLayer substrate enable the support for multiple specialized data link and interfaces with different communication characteristics and limited (or inexistent) monitoring capabilities. Internal AFRL and industry efforts (TacLink™) have investigated this problem and created specialized hardware devices for legacy systems. While these devices provide a common interface to different tactical systems, the access to the interface and interactions with the link are still delegated to the applications. The XLayer communications substrate helps to mitigate the problem by seamlessly assigning an IP-like interface to serial legacy system and by creating a common underlying routing infrastructure based on node IDs. This capability enables the seamless integration with different systems while still leveraging their unique capabilities as much as possible, without requiring link-specific changes on application behavior.

2.7 Dynamic Gateway Selection

Dynamically interfacing between multiple disjoint networks is also an important capability for tactical IMS support. Disparate networks in the battlefield may rely on different communications systems, routing and discovery protocols that are often incompatible with one another. The common approach to address the problem and provide interoperability is to rely on pre-defined gateways nodes capable to bridge communications across the different networks.

Gateway nodes are often realized by a system with multiple radios and communication interfaces capable to bridge across the different networks. The allocation of gateways is often part of a mission planning phase and generally static through the life of the mission, effectively creating so partial fixed 'infrastructure' connecting tactical sub-networks.

A more flexible approach to the problem is to enable the dynamic establishment of gateway nodes across multiple, disparate networks possibly running heterogeneous routing protocols. In [6], the authors have proposed a cross-layer approach to the dynamic gateway selection problem, supporting seamless and effective cross-domain routing between different networks. Seamless cross-domain routing requires at least three support capabilities that are cross-layer in nature.

- Nodes must be able to detect (at the RF level) the present of nearby network and appropriate exchange data frames, which is often associated with compatibility requirements at the physical and MAC layers.
- Nodes must be able to agree on common gateways and common protocols for information exchange, which requires a configurable layer 3, capable to leverage the information detected by the lower layers.
- Selected gateway nodes must be able to efficiently represent and share topology and route information across the different networks, which must be adaptive to IMS requirements for redundancy, and resource usation.

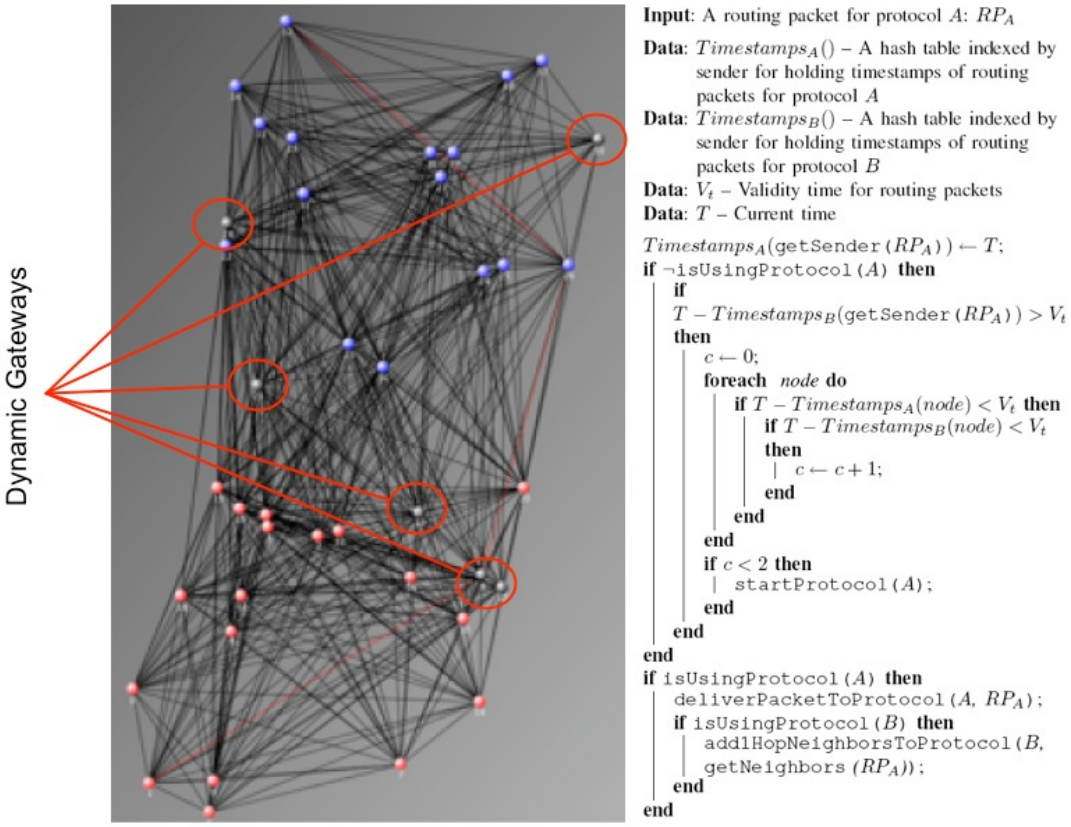

Figure 7. A Cross-Layer Dynamic Gateway Selection Algorithm

Our technical approach to support this capability (as described in [6]) relies on the XLayer communications substrate to enable the detection between networks, the gateway selection and the cross-domain route construction protocols. As illustrated in Figure 7, the gateway selection algorithm chooses more than one gateway to enable multiple bridge points across the different networks. The number of gateways can be specified by overlay applications and middleware either explicitly or through an indirect measure of reliability requirement, in which case the local topology is used by the cross-layer to ensure a minimum separation between selected gateways. In the illustrated example, the algorithm was selecting the maximum number of gateway points with non-redundant immediate neighbor so they are spread across the boundaries of the two networks to mitigate the effects of a localized failure (for instance due to Jamming).

Figure 7 also shows the pseudo code of the selection process, which can be configured by the overlay applications. While in this example, the selection algorithm is being applied to support cross-domain routing, the same capability could be leveraged to enable redundant services allocation across heterogeneous networks, without requiring full topology specification or disclosure on either side of the network, for more details on the protocol please refer to [6,7].

2.8 Adaptive Multi-Path Data Flows

With the support of multi-interface nodes in the scenario, a natural consequence is the availability of multiple data links between platforms at the local (one-hop) level, and increased complexity in the multipath end-to-end connections between. The JCAN also provides a dual-path support capability for QoS Management [7]. The system builds on the SCPS protocol and current multipath routing capabilities to balance data flows across multiple parallel data links to QoS support. In their technical report, the authors also recommend that information associated with multi-path routing and information be exposed to application proxies to enable adaptability and control.

The XLayer API for multi-path support does allow the IMS to specify the broad characteristics of the aggregated data channel in terms of reliability versus capability. For example, on a dual link scenario (e.g. 2.4GH and 900MHz radios) the IMS may choose between reliability and capacity to influence how the XLayer would distribute messages across each link. As throughput over each link is independently monitored by the XLayer substrate, the data flow automatically

adapts the usation between links, for instance in the presence of an external interference source (i.e. jammer), to comply with IMS requirements.

Currently, as illustrated in our previous example, the enforcement happens on a link-level basis, between every two hops in the complete data path. As part of our future development plans, we will incorporate end-to-end measurements of the data flow, to make decisions about link allocation at the local level. In a separate collaborative effort, we are investigating the integration of the cross-layer capabilities with JCAN, for enhanced, IMS-driven QoS-enabled data dissemination.

3. JOINT CAPABILITIY EXPERIMENTATION

The capabilities described in this paper have been demonstrated in isolation in a number of exercises and small-scale scenarios including the Army C4ISR OTM. Currently, the AFRL is sponsoring a number of research efforts to integrate and extend this research into a joint capability to be demonstrated in a relevant tactical information management scenario. As part of this effort, a large-scale experimentation is being prepared to evaluate and demonstrate AIMS, with integrated Federation and QoS Capabilities.

3.1 The AIMS Experiment

The AIMS Experiment will integrate the Federation and QED capabilities into Phoenix and Apollo and evaluate that in a realistic context. The experiment will involve a J-STARS platform, a Global Hawk platform, a ground station (e.g., a TAC-P handling close air support), and an AOC (Air Operations Center). These nodes will be emulated on an experimental testbed, which will also emulate the wireless network connectivity between the nodes.

The current prototype implementation is based on the Apollo implementation of the JBI, which has been extended by Northrop Grumman to realize the AIMS platform. This was driven partly by the monolithic nature of Apollo, which was not well suited to the needs of embedded and airborne environments. The new Phoenix architecture is Services-based, and supports a more component-oriented approach to information management. This will allow AIMS to pick and choose the specific capabilities (services) from the available set, as well as to add new capabilities in the form of services into the Phoenix architecture. Two versions of Phoenix are planned – a traditional Web Services based implementation targeted towards the enterprise and a lightweight, tactical implementation. The goal is to use the Phoenix lightweight implementation, called Fawkes, with the AIMS experiment, with the Apollo implementation being the fallback.

There are three goals for the AIMS experiment. The first goal is a capability demonstration, which involves integration of the Federation services into AIMS. If successful, this will provide transparent pub/sub/query capabilities to any client attached to any of the IMS operating in the experiment. We envision at least three instances of Phoenix – one at the AOC, one on the Global Hawk, and one on the J-STARS, which the ground station attaching via a tactical radio link to the J-STARS. In terms of evaluation, we will test the ability for the ground station to perform pub/sub/query operations that will result in data being pushed and pulled from the J-STARS, the Global Hawk, and the AOC platforms.

The second goal is to measure the efficiency of the Federation service, in terms of the overhead in bandwidth, processing, memory, and storage to provide the capabilities of federation. We will measure the overhead to establish and maintain the federation, as well as the overhead and latency in handling remote pub/sub/query. We will also evaluate the improvement of federation performance given the dynamic adaptations realized by the Federation Service.

The third goal is to integrate the QoS management capabilities that are part of the QED project into AIMS, and measure the improvement in terms of the timeliness of the data and other relevant measures. Given that the wireless links between the three AIMS instances (AOC, Global Hawk, J-STARS) are unreliable and bandwidth constrained, QoS management is important to maximize the capability and utility of the system. Moreover, the wireless link between the ground station and the J-STARS is even more bandwidth constrained. We will measure the improvement in performance of the AIMS system by adding the QoS capabilities.

4. CONCLUSIONS

In the last few years a significant amount of research efforts have focuses on building services and middleware for tactical network environments. In most cases, the approaches and techniques applied by such system to address the demanding requirements of the tactical environment tend to re-create customized (and often proprietary) services and protocols for their own use. In the last few years, a collaborative effort between industry and academia, lead and largely

sponsored by the Air Force Research Laboratory, has proposed the investigation of the common properties and capabilities required to support complex information management systems capabilities in tactical network environments.

The combination of multiple research projects in the last few year and technologies developed as part of these efforts has yielded a set of capabilities that is maturing to eventually provide the means to allow applications to seamlessly and effortlessly interface with very complex and dynamic communication environments, leading to the development of a new generation of highly adaptable, efficient and robust software infrastructures for military applications.

In this paper we have described some of the key capabilities being developed and tested as part of these efforts. While still a work in progress, most of the technologies described in this work have been demonstrated and evaluated in isolation in joint exercises with the Army Research Laboratory and the Air Force Research Laboratory. Some of the technologies described in this work are currently being integrated for a large-scale demonstration in support of the Advanced Information Management Systems (AIMS). It is our belief that collectively, a number of these capabilities will evolve to enable the successful deployment and operation of information management systems in tactical environments.

REFERENCES

1. Scientific Advisory Board, "Building the Joint Battlespace Infosphere Volume 1: Summary," SAB-TR-99-02, 2000.

2. Scientific Advisory Board, "Report on Building the Joint Battlespace Infosphere Volume 2: Interactive Information Technologies," SAB-TR-99-02, 1999.

3. Carvalho, M., Suri, N., Arguedas, M., Rebeschini, M., and Breedy, M. A Cross-Layer Communications Framework for Tactical Environments. In Proceedings of the 2006 IEEE Military Communications Conference (MILCOM 2006), October 2006, Washington, D.C.

4. Tortonesi, M., Stefanelli, C., Suri, N., Arguedas, M., and Breedy, M. Mockets: A Novel Message-oriented Communication Middleware for the Wireless Internet, in *Proceedings of International Conference on Wireless Information Networks and Systems (WINSYS 2006)*, Setúbal, Portugal, August 2006.

5. 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 IEEE Workshop on Policy 2008*, IEEE Press.

6. Carvalho, Marco, Granados, Adrian, Naqvi, Waseem, Brothers, Alfred, Hanna, James P. and Turck, Kurt, A Cross-Layer Communications Substrate for Tactical Information Management Systems, in: Military Communications Conference (MILCOM), IEEE, San Diego, CA, 2008

7. Carvalho, M., Perez, C., Granados, A., Dynamic Gateway Selection for Cross-Domain Routing with the XLayer Communications Substrate, submitted for publication at the Second International Conference on Cross-Layer Design, June, 2009.

8. Baskinger, Patricia, Card, Stuart, Zabele, Steve and Chruscicki, Mary Carol, Information for Global Reach, Northrop Grumman IT, TASC, 2007

9. Laouiti, A., Jacquet, P., Minet, P., Viennot, L., Clausen, T. and Adjih, C., "Multicast optimized link state routing," INRIA Rocquencourt, Tech. Rep., February 2003. [Online]. Available: ftp://ftp.inria.fr/INRIA/publication/publi-pdf/RR/RR-4721.pdf

10. Jie Wu and Hailan Li. On calculating connected dominating set for e_cient routing in ad hoc wireless networks. In DIALM '99: Proceedings of the 3rd international workshop on Discrete algorithms and methods for mobile computing and communications, pages 7-14, New York, NY, USA, 1999. ACM

11. Suri, N., Benincasa, G., Formaggi, S., Winkler, R., Choy, S., Kovach, J., and Tokarcik, L. 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).