Invited Paper: Network Management Architecture for the Objective Airborne Network

MILCOM Paper Abstract ID 1270

Doug Willard, 24 June 2004

Abstract - The objective airborne network (AN) will use a heterogeneous set of physical links (RF, Optical/Laser, and SATCOM) to interconnect terrestrial, space and highly mobile airborne platforms. The primary communications resources of the network will be the airborne platforms themselves, which will self-form into a network with a dynamic topology – i.e., a mobile ad hoc network. As a war-fighting asset, the objective AN should provide commanders the capability to ascertain the network's operational health and status – i.e., network situational awareness. Additionally, AN communications resources should be configurable to meet the commanders' operational objectives. These operational requirements are typically satisfied in terrestrial, wire-line networks by network management (NM) and policy-based network management (PBNM) capabilities. However, management of mobile ad hoc networks is an emerging research area facing many challenges: application of the NM Architectures for terrestrial wire-line networks is impractical due to reliance on dedicated, terrestrial-based servers and dependence on static network topologies. This paper identifies management challenges of the AN and outlines an architecture to address these challenges. The proposed architecture is then used to frame the critical research and technological needs the military communications community should address to enable network management of the future AN. This paper was invited for the Airborne Networking session by Kenneth Stranc, Session Organizer.

Introduction: Drivers of the AN Management Architecture

While much attention has been devoted recently to the research and design of routing protocols for ad hoc networks, there has been very limited attention paid to delivering network management over these dynamic networks. As can be imagined, conducting network management over a dynamic network with changing topology and bandwidth-constrained links has many challenges. Before a practical architecture can be formulated, it is important to first review these challenges and the implications to any NM architecture that would be applied to the AN:

1. Maintaining NM Services through Dynamic Networking Conditions: A general requirement stemming from the nature of dynamic (ad hoc) networks is that the network must self-form and self-configure. After the network self-forms, it may autonomously merge with other sub-nets or partition, and nodes may dynamically join or exit the network. The implication stemming from these mobility dynamics is that the NM architecture will have to dynamically adapt to the dynamic topology changes to deliver and maintain NM services across the mobile network. Thus, a dynamic and adaptive architecture is required, rather than the static ones applied to terrestrial, wire-line networks.

2. Efficiency: The NM architecture applied to the AN will be confronted by significant efficiency demands. Maintaining the integrity of a NM architecture across a dynamic topology will require a higher degree of overhead when compared to static, terrestrial networks. Yet AN links will be bandwidth limited, and of variable quality; the dynamic nature of highly mobile airborne platforms will result in occasions of link outages and degraded link quality. These constraints make it critical that any overhead required to adapt and maintain the NM architecture not overwhelm the data traffic. Additionally, network management transactions must also be efficient, and balanced in terms of the "cost" relative to the resulting benefit of the transaction.

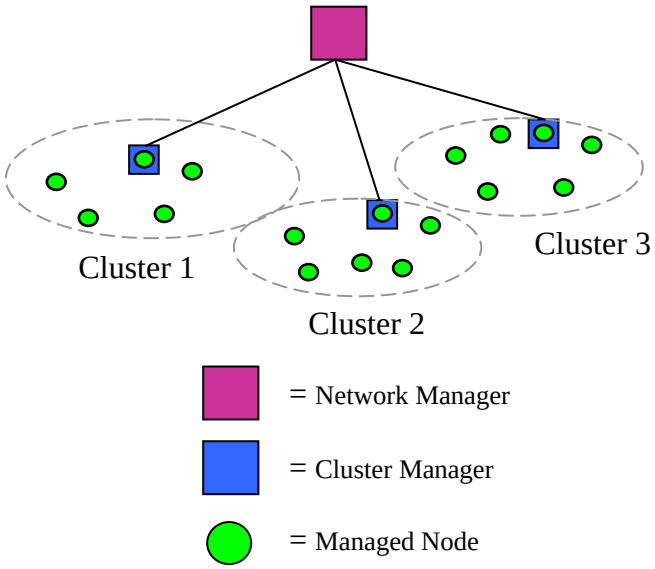
3. Autonomous, Disconnected Operations: Airborne operations will span the breath of operations, including autonomous operations without connectivity to ground nodes. The diversity of airborne network operations, and the potential that the AN will not have connectivity to ground nodes implies that the target NM architecture for the AN must be operate autonomously, without

connectivity to ground nodes. The implication here is that the AN NM architecture must make provisions to supply its own services from airborne locations.

The challenges enumerated above make application of current NM architectures impractical due to their reliance on dedicated, terrestrial-based servers and dependence on a static network topology. Rather, these challenges drive service-oriented capabilities such as NM away from the centralized architectures used in terrestrial applications to semi-distributed architectures that can better adapt to the challenges of airborne networking. One means of achieving a distributed architecture is by applying the concept of clustering. Various researchers have proposed cluster-based architectures to deliver a range of capabilities across ad hoc networks – including routing, QoS, and network management. The major components and features of a cluster-based management architecture, as it would apply to network management, are described below.

Cluster-Based Management Architecture

Cluster-based architectures have been proposed in recent literature [*Chen, ANMP*], [*Shen, An Adaptive Management Architecture forAd Hoc Networks*], and [*Phanse, Protocol Support for PBNM of Ad Hoc Networks*] as a means to deliver management services over ad hoc networks. Cluster-based management architectures group individual nodes into clusters that are managed by a cluster *head*, or *cluster manager*. The cluster managers are in turn managed by a network manager. The figure below illustrates the logical relationship between the components. The subsections below describe the functionality and features of these components in the context of the AN.



Network Manager

The Network Manager executes management applications that monitor and control the AN. As such, it will provide visualization of AN situation awareness, and provide a focal point from which to conduct general monitoring and control. The NM must be located at a semi-persistent node in the network, whether in the air or on the ground. However, as opposed to a conventional architecture, in which a centralized network manager interacts directly with all agents, the AN NM distributes management policies and guidance to its Cluster Managers.

Cluster Managers

Cluster managers occupy a middle tier in the management architecture, distributing control and configuration commands to managed nodes in accordance with the policies and directives of the Network Manager. Cluster managers also act as proxies to aggregate and filter information -- based on cost-benefit examination -- from the cluster's nodes to the Network Manager. Thus, cluster managers provide a type of proxy *service* between the network manager and the managed nodes. However, in conducting this service, it is critical that cluster managers maximize the service availability to all nodes in spite of the AN's dynamic network changes and nodal mobility. One fundamental requirement is that the architecture should be able to adapt to the loss of any cluster manager. Three processes are proposed to satisfy the required adaptation features: cluster manager election, cluster manager advertisement/discovery, and cluster maintenance.

Cluster Manager Election

One of the attributes of a distributed services architecture is the ability of multiple (and in some cases, all) nodes to act in the capacity of "a server". References [*Toner, Self-Organising Node Address Management in Ad Hoc Networks*], and [*Jeong, DNS Name Service for IPv6 Mobile Ad Hoc Networks*], among others, propose service capability be instantiated across a majority of (and in some cases all) nodes to deliver services across ad hoc networks. Thus, to deliver cluster management services, multiple nodes are capable of serving the role of the cluster manager. Whether or not this sub-set of network nodes serve as cluster managers is determined by a cluster manager election process. As the network self-forms, nodes that can act as a cluster manager are elected (or selected) by an election protocol, and take on the server capability. The objective in selecting cluster managers is to minimize protocol overhead while maximizing service availability. Continued invocation of thee election process after the network self-forms enables the architecture to continuously adapt to the network's dynamic topology. Thus, as the topology changes, the nodes serving the role as cluster managers will also change to maximize the availability of the NM proxy service. For instance, if a node leaves or becomes inoperable, an election process ensues to select a new cluster manager. If two sub-nets, previously disconnected and employing their own cluster managers merge, the election/selection process reconciles the redundancy. Thus, the election of cluster managers is dynamic and conducted either on a periodic or event-driven basis to adapt to the dynamic topology changes.

Cluster Manager Discovery/Advertisement

After cluster managers have been elected, they implement an *advertisement* feature to announce their role as cluster managers to the network. A service *discovery* process often compliments this advertisement process. The discovery process is employed by nodes which are in search of a server (i.e., cluster manager), such as those that have recently joined the network. Various service advertisement/discovery protocols exist for terrestrial wire-line networks (for instance, Service Location Protocol (SLP)). These approaches typically use a broadcast or some form of multi-cast suitable for wire-line networks; however, given the bandwidth-constrained AN links, these protocols are most likely not directly applicable. Chief among the issues is the need to minimize service advertisement overhead. Various features may be employed to reduce overhead, including constraining the broadcast announcement to *n*-hops, using MANET protocol multi-casts rather than broadcasts, and enacting the announcement only upon trap-driven events. Sources [*Chen*], and [*Phanse*] propose various approaches to service discovery and advertisement.

Cluster Maintenance

Cluster managers conduct a cluster maintenance process to manage the nodal membership, control the general cluster structure, and adapt management functions to the environmental conditions of the cluster. Like cluster manager election, the performance objective in cluster management is to minimize protocol overhead while maximizing service availability. Sources [*Chen*], [*Shen*], and [*Phanse*] outline different approaches to conduct cluster maintenance. These approaches range from the simple *n*-hop clustering utilized in [Phanse], to the proposal in [Shen] of a sophisticated utility function to enable dynamic cluster adaptation using environmental inputs and cost-benefit criteria.

Intelligent Nodal Agents

In the AN management architecture, managed nodes must be imparted with a high degree of "intelligence" to minimize unnecessary management overhead across bandwidth-constrained AN links. Imparting local intelligence within nodes enables a reduction in unnecessary management overhead that occurs in centralized architectures with "dumb" agents. Rather than conducting centralized polling from the network manager to collect data, intelligent agents will conduct local data collection, event analysis, and report aggregation before forwarding to the cluster manager. In generating reports, intelligent nodal agents may conduct cost-benefit assessments on transactions with the Cluster Managers – taking into account the link's available bandwidth, node's emission control (EMCON) state, importance and timeliness of event reporting, etc. Additional intelligence features include the ability to conduct local problem resolution. This capability may be augmented via the use of mobile code technology. In mobile code technology, rather than repeatedly polling an agent to gather the data necessary to conduct a NM decision at the manager, the decision logic (i.e., the mobile agent code) is sent from the manager to the agent and applied locally to the data at the agent [*Bohoris, Evaluation…*], [*Liotta, On the Performance…*].

Policy Based Network Management Framework

One of the operational requirements of the AN is that its communications resources be configurable to meet the commanders' operational objectives. This can be particularly challenging in an ad hoc network in which subscriber nodes that also provide the network infrastructure. Subscriber nodes must donate some portion of their communications resources to support *inter*-network transit traffic – i.e., traffic that neither originates nor terminates at the platform. This *inter*-network transit traffic flow must be balanced with traffic flows that originate or terminate at the node. Policy based network management is a means for applying policies to achieve the balance of flows in accordance with organizational objectives. However, before a practical PBNM architecture can be formulated for the AN, it is advantageous to review the approach applied to enforcement of terrestrial networks.

IETF-Proposed PBNM Architecture

The IETF Policy Framework Working Group has developed a policy management architecture that is considered the best approach for policy management on the Internet. It includes the following components:

- Policy Server – A graphical user interface for specifying, editing, and administering policy.
- Policy Repository – A device used to store and retrieve policy information.
- PDP (policy decision point) – A resource manager or policy server that is responsible for handling events and making decisions based on those events and updating the PEP configuration appropriately.
- PEP (policy enforcement point) – Network devices such as routers, firewalls, and hosts that enforce the policies received from the PDP.

In most implementations of the framework, the Policy Server, Policy Repository, and PDP are collocated and may potentially be hosted within the same physical device. The discussion of the framework below assumes this consolidation of system components. For the sake of conciseness, this consolidation of functions will be termed *Policy Manager* in the ensuing discussion.

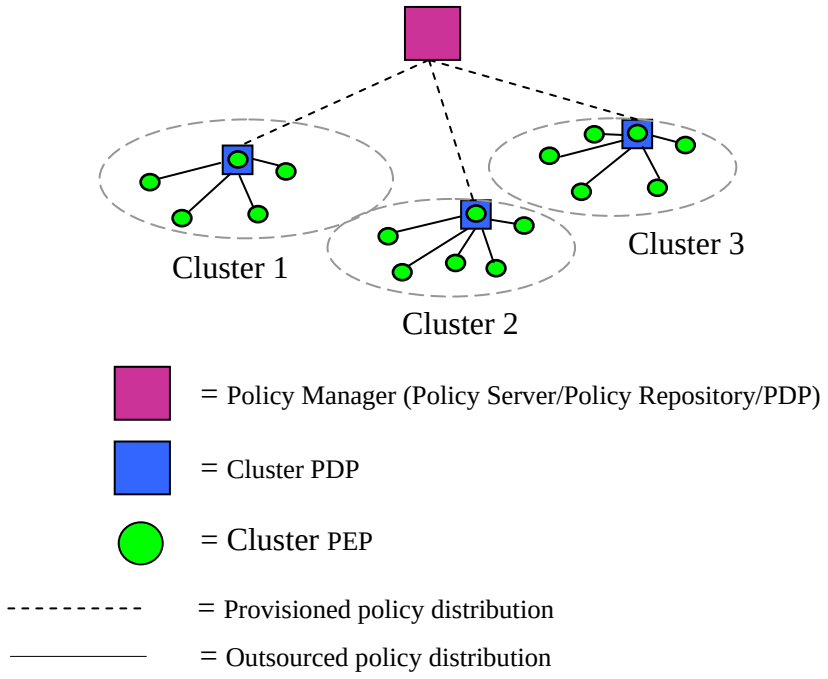
Adaptation of IETF Framework for the AN

The general IETF framework may be adapted to the policy requirements of the AN. In the AN-adapted framework, a ground-based resource planner would formulate high-level airborne networking policies -- that is, formulation of the relatively static, high-level specifications of the desired behavior of flows. These sets of high-level policies would be downloaded into the airborne- or ground-based Policy Manager prior to operations. In addition to the Policy Server/PDP/Repository and PEPs outlined in the IETF framework, a

middle tier of elements -- termed *cluster* PDPs – is required for adaptation to the dynamic topology of the AN. These cluster PDPs are analogous to the cluster managers described within the NM architecture, and utilize the same processes: server election, server advertisement/discovery, and cluster maintenance. And rather than forming separate, independent NM and PBNM architectures – with NM and PBNM employing separate physical architectures and maintenance transactions – a unified, common architecture is proposed to achieve efficiency gains across the AN. Thus, PBNM elements are overlaid onto the cluster-based network management architecture and piggy-back on the same NM server election, server advertisement/discovery, and cluster maintenance processes used by the NM elements. Specific functionality of PBNM elements are discussed below.

Policy Manager

The Policy Manager is responsible for distributing policies to the cluster PDPs. Policy managed services may include quality of service, traffic engineering features, and security attributes. Each service would employ a common set of policies, termed a Policy Information Base (PIB). There are two models for distributing policy: outsourcing, and delegated provisioning. In outsourced distribution, all policy decisions are conducted at the PDP. In delegated provisioning, policy directives may be defined in broader terms, with flexibility for local policy interpretation based on local events and conditions [*Intel Labs, Simplifying Support of New Network Services Using COPS-PR*]. A hybrid solution for policy distribution, using both outsourcing and provisioning, would provide the flexibility required for the AN. The outsourced model provides the option for explicit control of particular PEPs. The provisioning model is recommended at cluster PDPs to minimize signaling overhead and enable a degree of autonomy required for provisioning semi-persistent cluster PDPs. The figure below illustrates the PBNM overlay onto the NM cluster architecture, and use of the hybrid approach to policy distribution.



Cluster PDP

Cluster PDPs are provisioned to act as mid-tier PDPs, interpreting and distributing policies from the Policy Manager to their cluster nodes (Cluster PEPs). Because each cluster manager acts as a local PDP for its cluster PEPs, the node is imparted with a degree of self-sufficiency required in semi-autonomous cluster operations. Sources [*Phanse, Extending PBNM to Ad Hoc Networks*] and [*Phanse, Protocol*] provide initial research and experimentation in the area of policy management for ad hoc networks.

Cluster PEP

Cluster PEPs enforce the policies received from the Cluster PDP. Similar to the Intelligent NM Agents, cluster PEPs may conduct cost-benefit assessments on transactions with the Cluster PDPs – taking into account the link's available bandwidth, node's emission control (EMCON) state, importance and timeliness of a policy request, etc. Where possible, Cluster PEPs will consolidate policy requests from network devices such as routers, firewalls, and hosts to minimize transactions between Cluster PDP and policy-managed elements.

Critical Research and Technology Needs

While a wide array of technological "gaps" prohibit implementation of an airborne network with today's technology, the following are regarded as the shortfalls requiring a significant research and development to enable an adaptive management capability for the AN.

Election, Advertisement, and Discovery Protocols

To support the spontaneous, self-forming features of the AN, the network management architecture will require autonomous election of cluster managers and advertisement/discovery of those managers within the network. After the network self-forms, continued invocation of these processes enable the NM architecture to adapt to the network's dynamic topology changes. Some proprietary and standards-based solutions for automated service discovery exist for fixed, wire-line networks (Service Location Protocol, Salutation Protocol, etc). However, these most likely would not be appropriate for dynamic topology networks. One issue is the problem of broadcast flooding over ad hoc networks with bandwidth-constrained links. The selected service discovery methods would need to constrain the broadcast function in some fashion to avoid redundant flooding and inefficient use of bandwidth resources. Some potential options include use of MANET protocol multi-cast and/or constrained (hop-limited) broadcasts. This area warrants particular attention to achieve self-forming, adaptive services for the airborne network.

Adaptive Clustering Protocol for AN Topology Dynamics

The main concept behind cluster management is to convert a traditionally centralized process into a semi-distributed process that can adapt to dynamic network changes. The performance objective in maintenance of network clusters is to minimize protocol overhead between client and server while maximizing management service availability. Selection of cluster size is an important parameter in forming and maintaining clusters. Clusters that are too large suffer from an excess of overhead due to collection of data from a large number of clients. Networks with clusters that are too small suffer from an excess of overhead in cluster maintenance traffic [*Phanse, Protocol Support*]. Additional factors that impact cluster maintenance include, among others: relative node speed, cluster density, mobility characteristics, etc. Various recent research endeavors have proposed cluster management schemes. However, none of these have been formally implemented, or evaluated against the particular attributes (relative node speed, cluster density, mobility characteristics) of a military airborne network.

Security Architecture for Secure Management Transactions

Currently, a number of different security constructs exist that can be applied to today's wire-line NM transactions, including public key technologies, security protocols including IPSec enabled virtual private networks (VPN), Transport layer Security (TLS), Secure Socket Layer (SSL), as well as protocols with built-in security features, such as the SNMPv3 User Security Module. These approaches were designed upon the premise that dedicated, terrestrial-based security resources would be available to support these security services. However, the tenet that the AN be able to operate disconnected from terrestrially-based services makes application of these approaches in their present form difficult, if not impossible, to implement [*Rush, MITRE White Paper*]. Thus, a significant gap confronting the AN architecture in general

-- and the AN NM architecture in particular -- is how to secure administrative transactions over a disconnected, dynamically changing network.

Summary

In this paper, we identified the specific challenges to managing the AN. We examined the implications of these challenges to any architecture that would be applied to manage the AN. In view of these implications (i.e., architectural drivers), we have proposed that a cluster-based architecture be applied to satisfy the required adaptation required of the NM capability for the AN. However, there exist an array of technological “gaps” that currently prevent implementation of such an architecture. These “gaps” were identified and briefly discussed in the hope that by doing so would encourage the Military Communications community to propose suitable solutions to these gaps, thus ultimately enabling network management of the AN.