Role of the Mobile IPv6 in DoD's Service Oriented Architecture

Carl Williams
Derya Cansever
SI International
Reston VA

and

Junaid Islam
Piano Networks
San Jose CA

ABSTRACT

Service Oriented Architecture (SOA) is a new paradigm for organizing and utilizing distributed computing resources. When implementing SOAs for the DoD, it is critical that warfighters have access to mission critical services from any location on the global. Unfortunately present SOA systems assume a static, reliable network. Tactical networks are composed of mobile network elements with variable connectivity and are thus inherently "unreliable". Usage of Mobile IPv6 as a connectivity strategy for SOAs creates a disruption tolerant network that ensures mission success.

INTRODUCTION

Future battlefield networks present several critical challenges. The networks must be self-configuring and self-maintaining so that they can be rapidly deployed and quickly reorganized when needed. All elements must be highly mobile and survivable, including routers that make up the communications infrastructure. Entire networks may move, or nodes and links may be added to an existing network. As networks merge and split, dynamic border routers must adjust route information dynamically. Available bandwidth must be used efficiently, and information must be disseminated rapidly, so that the right information is available at the right place and time. DoD battlefield deployments pose stringent requirements for security and reliability. Links are susceptible to failures because of mobility of nodes, or loss of connectivity due to unreliability of wireless links or terrain effects. Nodes may fail because they have been destroyed during combat. Such systems need rapid re-configuration to activate key network functionality in event of failures. The most prevalent services of a these future battlefield network environments are mission critical real-time multimedia multi-party collaborative applications that allow commanders and war-fighters to receive "live" view of the battlefield and adapt their strategy accordingly, and communicate it to the war-fighters, robots, and smart weapons in a timely manner.

Service Oriented Architectures allows warfighters, commanders and civilian forces to reach across their distributed and disparate data sources for immediate, actionable information. Service Oriented Architectures are by definition distributed. The purpose of a service is to communicate remotely with another service, and fuse data. The rise of a ubiquitous service orientated computing has brought new opportunity for productivity and new challenges for SOA architects and designers. As the DoD deploys multiple service instances, they will need to provide an infrastructure to manage, secure, mediate, and govern these resources in a manner that is transparent to the warfighter.

To meet the connectivity challenges of the DoD, the use of Mobile IPv6 is introduced into SOA implementation. The paper outlines how a Mobile IPv6 based SOA can enable interoperability across enterprise and tactical architectures. More importantly, the paper introduces a new concept that enables SOAs to publish their services as discoverable resources to mobile warfighters and enable them to access services irrespective of connectivity. Finally, the paper details how Mobile IPv6 enables end-to-end security across heterogeneous environments and applications.

MOBILE IPV6 BASED SOA NETWORKS

Services Oriented Architectures (SOA) holds the promise of improving DoD mission capability and agility. However, there is controversy as to what a SOA is and how to implement it. It is clear that SOA require a network centric solution to enable connectivity. SOA's decentralized application environment provides a great deal of flexibility for the various service units, but it also creates difficulty in managing the varying security levels and the diversity required by the different services.

Net-centric operations require that connectivity be ubiquitous – enabling IP nodes or routers to change their physical point of attachment from one network to another in a seamless manner. One solution to enable SOAs to function in a tactical environment is IPv6. However IPv6 by itself is unable to meet the demands of mobile connectivity over high loss links. To meet the requirement of a "battlefield SOA", Mobile IP extensions are added to IPv6 enabling ubiquitous connectivity for all IP devices. The end-to-end connectivity of IPv6 when extended with the features of Mobile IP provides a disruption tolerant network for user nodes and routers no matter where it may move.

SERVICE DISCOVERY CHALLENGE

In a Net-Centric environment, Service Discovery plays a critical infrastructure role:

- Discovery allows service producers to publish / advertise service definitions, descriptions, metadata, and accessibility. The information producers may include Web services (such as service-enabled target tracking applications), data repositories (such as a Coalition Shared Database), devices (such as sensor platforms), or even non-technical business functions (such as a helpdesk for technical support).
- It allows service consumers to discover service information as advertised by producers. The information consumers may include thick clients (such as service-enabled Command and Control applications), thin clients (such as Web browsers), or devices (such as PDAs).
- It should allow information developers to transparently enhance discovery, retrieval, and publishing services without interrupting normal business operations. It should allow other service producers to discover services to integrate at design or run-time to create other composite services.
- Along with other Net-centric Enterprise Service components, Service Discovery is responsible for getting the right information to the right people at the right time in the Net-Centric environment.

Figure 1 below provides an overall illustration of SOA Service Discovery. Service Discovery is often compared to the common "Yellow Pages" which organizes business listings by the product or service.

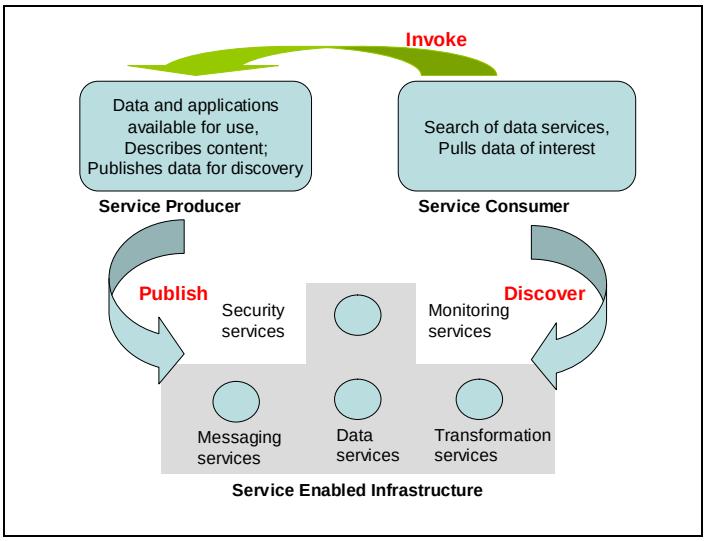

Figure 1. DoD Net-centric SOA core

The United States Department of Defense governs the Army, Air Force, Navy, and a host of supporting intelligence and logistics agencies. Collectively the supporting IT organization is the largest IT enterprises in the world. The DoD's systems are highly variable in their implementation details and the DoD requires a comprehensive approach to making its data assets visible.

As a result of this diversity, it is critical to implement service discovery as described in Figure 1 in a manner that is transparent to the highly variable characteristics of the different forces and agencies organizations. In addition, it is imperative that protocols, services, and methodologies are developed for performing real-time, disruption tolerant

discovery of publish-subscribe entities over WAN environments that will meet the Information Assurance (IA) requirements of the Global Information Grid (GIG). Each node is free to roam anywhere these links provide coverage, switching links as needed, without losing its unique IP address. In this respect, Mobile IPv6 based services will aid the DoD implementation of SOA architecture features. The functionality of publish (i.e. discover) and pull (i.e. retrieve) can be built upon Mobile IPv6 based primitives.

The transformation to network centric warfare requires seamless air-to-air, space, and ground connectivity. The IP communications systems required to provide this capability depend on end-to-end data channel that is secure. In addition, it must be portable across all wireless platforms and be independent of IP version type.

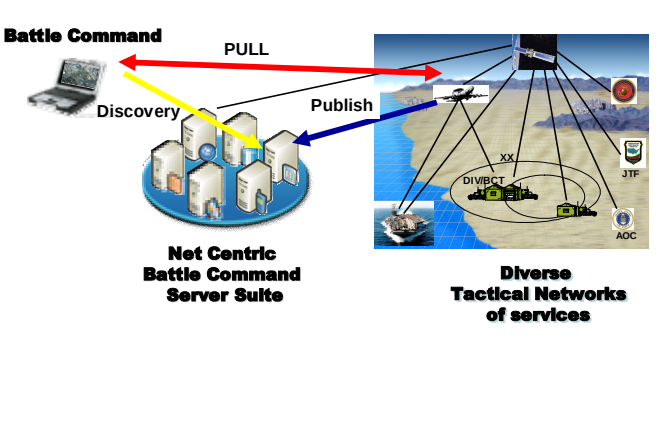

Figure 2. Mobile IPv6 Aiding Discovery and Access

Figure 2 illustrates the publication of data taken by some mobile aircraft. The data is published to those peers that should have access to this data. The battle commander will immediately learn of this data and in real-time pull this data for analysis. All of this is done over very diverse, fast changing environments.

DISTRUPTION-TOLERANT SERVICE, PUBLISH-SUBSCRIBE CAPABILITY

DoD and its various services (i.e., Navy, etc) real-time systems are increasingly adopting publish-subscribe middleware technology. Typically, these systems are limited to a local area network (LAN) environment such as a single combat system or as a single air, surface, or subsurface platform. Current real-time publish-subscribe technology does not support usage in a Wide Area Network (WAN) environment. In particular, the protocols used to dynamically locate data consumers and data providers generally require significant communication between participants. In a high loss WAN environment, excessive bandwidth consumption as well as the introduction of significant delays if an Enterprise style SOA is deployed in such an situation. New technology for discovery protocols, services and methodologies are required to resolve this problem. Additionally, all communication over the GIG must be protected. The information assurance mechanisms provided by the GIG backbone are in development and evolving. These mechanisms will likely be implemented at the network and transport layers. Because publish-subscribe middleware is generally used in a self-contained environment, mechanisms to validate the identity of data producers and consumers as well as the ability to associate classification data with the data transmitted have not been addressed by existing technologies and products.

In a publish/subscribe paradigm, user service discovery requires matching user preferences to available published services, e.g., a warfighter may want to find if there is tank support close by. This is a difficult problem when users are mobile, wirelessly connected to a network, and dynamically roaming in different environments. The magnitude of the problem increases with respect to the number of attributes for each user's preference criteria, as matches must be done in real-time. The Mobile IPv6 innovation described in this paper provides a real-time disruption-tolerant, publish-subscribe discovery capability in a WAN environment.

A disruption-tolerant "smart-push" mechanism based on Mobile IPv6 for sending data only to the systems that have a need for it is presented in Figure 3. In this figure a smart-push is invoked. Only those in the prescribed group of battle command participants will have access to the published data or services that is being pushed. The figure also illustrates the use of a COI (Common Community of Interest). COI is a means by which network assets and or network users

are segregated by some technological means for some established purpose. Mobile IPv6 COI's are set up to protect a Network infrastructure from a group or groups of users who are performing some esoteric functions. COI's are also designed to protect their user community from the rest of the enclave user population. Here they are used to group together warfighters and other DoD entities.

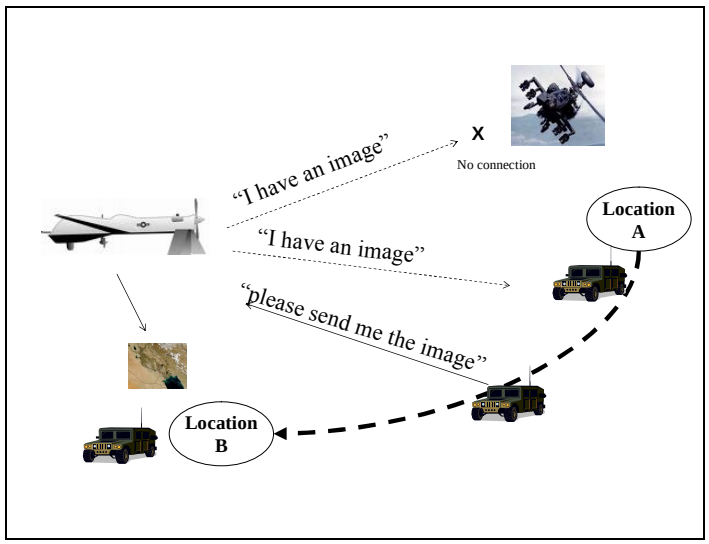

Figure 3. A "smart-push" mechanism using COI model

Here in Figure 3 the COI that is established is those participants in the noted battle command circle. When a "smart-push" is invoked, only those in the COI will receive this "push" data. A DoD COI can be defined as a collaborative group of war-fighters who must exchange information in pursuit of their shared goals, interests, missions or tactical processes and who therefore must have shared vocabulary for the information they exchange. It can be a logical or physical grouping of network devices or users with access to information that is not made available to the general DoD population on a LAN or the entire GIG infrastructure. A COI can be utilized to provide multiple levels of protection for a LAN or the GIG infrastructure from the activities within a COI. A COI can consist of a logical perimeter around the community (or enclave). It can allow for separate security management and operational direction. COI's generally do not dictate separate internal security policies (e.g., password policies, etc.) because they fall under the jurisdiction and management of the LAN or GIG owners (i.e., DISA). However, they can and often do have a laxed subset of the overall Network security policy.

Figure 4 describes a disruption-tolerant "smart-push" whereby some devices that are part of the same COI are on-line and others are off-line. Off-line being physically detached from the GIG and no communication path exists. At some point the off-line devices will come back on line. The commander who was performing the "smart-push" doesn't need to invoke the push facility again. For example, the data being pushed only needs to be pushed once. When devices that are part of the COI come back on-line the SOA architecture will detect this and immediately and proceed with pushing the data to those respective devices.

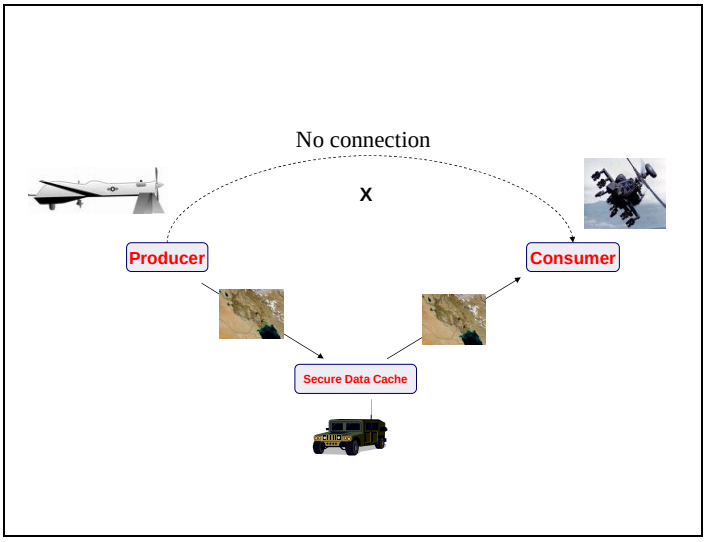

Figure 4. A disruption-tolerant "smart-push" mechanism

The method for detecting on-line and off-line by the SOA server suite is to use the Mobile IPv6 protocol with new innovative extensions that enable disruption tolerant networking. When those devices have no network connectivity, the SOA server suite will receive a Mobile IPv6 protocol message indicating that the device went off-line. When the device is back on-line, the Mobile IPv6 client will inform the SOA server suite of its availability at its new location and the "smart-push" can proceed.

Such a disruption-tolerant "smart-push/pull" enables the delivery of net-centric capability to the tactical level. This includes data pull or push flows to and

from the fox hole. It also includes dealing with the implications of managed services vs. government built services – Security, Competition and Integration with legacy applications and infrastructure.

It should be noted that as the Navy begins to leverage FORCEnet and the GIG, Mobile IPv6 publish-subscribe technology has the potential to play a significant role in distributed operations such as engage-on-remote, while helping to limit bandwidth consumption through a "smart-push" mechanism for sending data only once.

END-TO-END SECURITY FOR SOA OPERATIONS

For net-centric military operations to realize the linking of field resources together using Internet Protocol (IP)-based networking and provide highly mobile data sharing a security architecture an end-to-end security model is required. Today's common perimeter-based security models assume fairly constrained and static views of network composition, topology and trust models. While perimeter-based models can be hierarchically deployed (i.e., "defense in depth"), often at the lowest levels there are few explicit security mechanisms; instead relying on "local trust" at the subnet, or site level.

While middle-man network based security models could be thought of as the best common practices for today's networks, there are growing needs for new models of network composition, trust and security services. The growing importance and acceptance of nomadic devices (e.g., laptops, PDAs, IP phones, sensors), self organizing systems (e.g., mobile ad-hoc networks; service oriented software architectures; and peer-to-peer systems), environments with un-trusted local links (e.g., public wireless access points, multi-access residential broadband) may indicate that traditional perimeter (e.g., firewall) models are becoming obsolete. Moreover, as emerging threats will increase DoD missions on a global scale, the use of leased public bandwidth will grow.

With the adoption of Mobile IPv6, the opportunity exists to develop new end-to-end centric security architectures that distribute policy enforcement, security services, intrusion detection, etc. to multiple points in the network as required for the given deployment scenario. In such architectures, security policies can be defined at the finest granularity required. No longer would coarse site-wide security policies inhibit individual hosts from deploying new applications and services that need to be added for a mission. The implicit distributed security enforcement architecture could be realized in a hybrid manner, with some policies and services implemented in a perimeter model and others residing on individual mobile nodes (hosts).

Figure 5 presents a new security model whereby security policies are configured at the end hosts. The security policy and communication channel remain intact even though the end hosts may change their points of attachments from one network location to another – be it classified or unclassified. End-to-end encryption and secure channel enables sensitive data to be transferred over all types of networks even when the nodes or the entire network is moving.

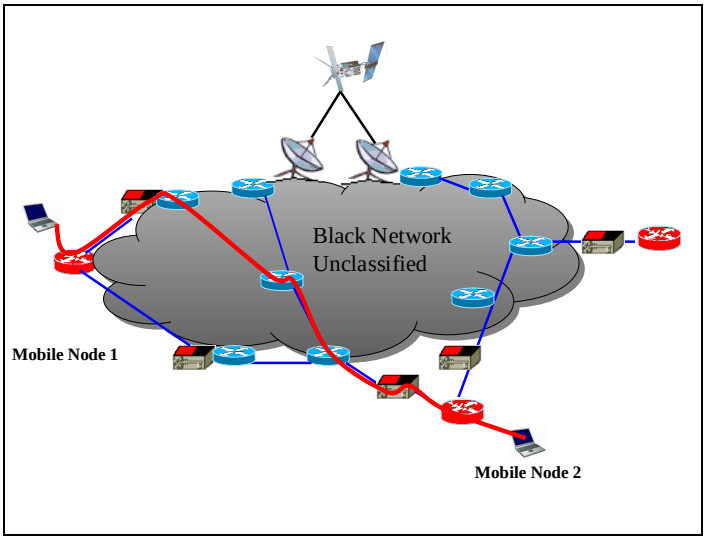

Figure 5. Mobile IPv6 end-to-end security model

In summary, the key security capabilities that Mobile IPv6 provides for can be enumerated as follows:

- End-to-end encryption of all traffic
- Global addressing & reachability
- Ubiquitous connectivity to mobile nodes or networks

CONCLUSION

To keep pace the changing nature of warfare the DoD realizes that their traditional software development tools are too slow and expensive to deliver the required services to the warfighter. A Mobile IPv6 based SOA creates a secure, agile, robust, dependable, interoperable data sharing environment for the warfighter.

By leveraging the powerful capabilities of Mobile IPv6 to enable the discovery and access of services while on the move, the DoD can unlock the full value of SOAs.

REFERENCES

[1] D. Johnson, C. E. Perkins, and J. Arkko, ``Mobility Support in IPv6", Request for Comments (Proposed Standard) 3775, Internet Engineering Task Force, June 2004.

[2] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[3] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[4] Piper, D., "The Internet IP Security Domain of Interpretation of ISAKMP", RFC 2407, November 1998.

[5] *DoD Net-Centric Data Strategy, DoD CIO office,* May 9, 2003.