[1]An Investigative Analysis of Information Assurance Issues Associated with the GIG's P&P Architecture

B.S. Farroha*[a], R.G. Cole[a], D.L. Farroha[b], A. DeSimone[c]
[a]Johns Hopkins University/Applied Physics Lab, 11100 Johns Hopkins Rd, Laurel, MD 21073
[b]Defense Intelligence Agency, Bolling AFB, Washington DC
[c]OASD/NII, 6000 Defense Pentagon, Washington, D.C.

Key Words: GIG, Precedence and Preemption, QoS, Networking, Information Assurance, Interoperability, Assured Services, DoD Communications, End-to-End Transport, Net-Centric

ABSTRACT

The Global Information Grid (GIG) is a collection of systems, programs and initiatives aimed at building a secure network and set of information capabilities modeled after the Internet. The GIG is expected to facilitate DoD's transformation by allowing warfighters, policy makers, and support personnel to engage in rapid decision making. The roadmap is designed to take advantage of converged services of voice, data, video, and imagery over common data links. The vision is to have commanders identify threats more effectively, make informed decisions, and respond with greater precision and lethality. The information advantage gained through the GIG and network-centric warfare (NCW) allows a warfighting force to achieve dramatically improved information positions, in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power.

The GIG Precedence and Preemption (P&P) requirements stem from the need to utilize scarce resources at critical times in the most effective way in support of national security, the intelligence community and the war-fighter. Information Assurance (IA) enables all information and data to be available end-to-end to support any mission without delay in accordance to the sensitivity of the task. Together, P&P and IA ensure data availability integrity, authentication, confidentiality, and non-repudiation.

This study addresses and analyzes the QoS and P & P requirements and architecture for the GIG.   Threat scenarios are presented and used to evaluate the reference architectures. The goal of the study is to assess the Information Assurance concerns associated with implementing Precedence and Preemption within the GIG and to guarantee an acceptable minimum level of security and protection for DoD networks.

1 Introduction

In support of national security, the intelligence community and the war-fighter the GIG Precedence and Preemption (P&P) requirements are critical to providing efficient means to communicate securely and reliably over the limited transport resources. Key to the uninterrupted flow and making the most efficient use of the network is providing awareness of information as well as Information Assurance (IA) within a commander's area of responsibility and providing the capability to dynamically adjust the priority of information flow based on the current operational environment. This analysis effort was conducted by the Quality of Service (QoS) P&P team in support of the OSD CIO's mission to develop an architecture for packet based transport service supporting the P&P operational

[1*] sam.farroha@jhuapl.edu: Phone 1 443 778-1692

requirements. The architectures proposed and developed by the P&P Team are still maturing. Further, the GIG P&P architecture is being reviewed by the user community and hence should not be considered as the final GIG architecture for P&P transport services. This paper discusses IA within the GIG P&P architecture.

2 Requirements Analysis

Achieving information superiority requires a Net-centric operational environment with the proposed Global Information Grid (GIG) providing an end-to-end set of information services, associated processes, and people to manage and provide the right information to the right user at the right time with appropriate protection across all DOD war fighting, intelligence and business domains. CJCSI 6215[3] provides a vision of the current requirements of the next generation systems

2.1 Precedence Levels

The envisioned precedence levels are based on current operational communications systems requirements. The current DoD priority levels will be adopted in the new system. The GIG will differ from other DoD infrastructure by being an all IP network where sessions are established and communication flows are based on next hop network characteristics. The approved priority levels are [3]:

1. FLASH OVERRIDE is considered a capability, not a level of precedence. Exercising this capability preempts calls of all other levels or precedence. Flash override messages should never be blocked.
2. FLASH messages preempt IMMEDIATE, PRIORITY, and ROUTINE messages. Some examples of FLASH calls include messages pertaining to C2 of military forces essential to defense and critical intelligence essential to national survival and communication of catastrophic events of national or international significance
3. IMMEDIATE messages preempt PRIORITY and ROUTINE messages and are reserved for communications pertaining to situations that gravely affect the security of U.S. and Allied forces.
4. PRIORITY messages preempt ROUTINE messages and are reserved for communications needing expeditious action by destination parties furnishing essential information for conducting Government operations.
5. The ROUTINE messages precedence applies to official Government communications that need rapid transmission by telephonic means, but do not need preferential handling. A ROUTINE call does not preempt any other call.

2.2 General P&P IA Needs

It is critical to address IA within the GIG. The following highlight the main aspects of IA from a GIG perspective:

- User authentication: The IP type network is based on users joining the network from static or dynamic physical locations. The dynamic physical location places a requirement on the user to identify and authenticate her/his identity to acquire the level of service they are allocated. Once the user is authenticated, they are allowed to establish sessions on the GIG to the highest priority level they are authorized [6]. The precedence level of the call is maintained for the duration of the call, which ends at the session termination time.
- Precedence level access: Defines who is allowed access to specific Precedence Levels. Note: The two end-points participating in a given session carry the Precedence Level as requested by the initiating party.
- Network survivability: This is based on different attack scenarios and the level of survivability in addition to mechanisms of defense. This is particularly important when working with heterogeneous networks that are interconnected and dependent on each other for end-to-end delivery.
- Network Robustness: Ensure that the network is robust against Denial of Service (DoS) attacks. The problem becomes more prominent when the attacker can masquerade as a high priority user.

- Network Forensics: The use of network forensics to identify, track and disable potential intruders.
- Management and Control: The use of management and control of high Precedence Levels to reduce the possibility of intentional or unintentional blocking the transport services. The overtaking of network controls by an enemy or even if the enemy can access the network and send streams of control messages requesting service from the controllers, then by simply flooding the controller with requests, the system's efficiency will be reduced.
- Header Encryption: The use of Header Encryption to mask user/priority level which might give an enemy an advantage. The mechanism by which decrypting/encrypting the headers to expose the priority and destination can reduce efficiency and robustness.
- Definition of the requirements and scenarios where the commander's intent and authority is clearly understood. The commander who is using an isolated system can establish and award priority level within his command to best serve his mission; however once connected to the GIG the system have to follow the globally established rule.
- Mechanisms to prevent spoofing, since the precedence is based on the initiator's address.

3 Attack Scenarios

The initial analysis focused on performance in the presence of benign situations as well as Denial of Service (DoS) attacks by internal or external entities that flood the network with messages of a high priority. Specifications have been addressed that allow for network forensics to identify and isolate offenders. The fundamental issue is that anytime we add a capability to utilize the higher priority of the transport, it opens a hole for intruders to highjack the system with more devastating effects on the capability, however the lack of such capabilities will cause the demise of the system. The utilization of defense in depth is being considered as a key solution. Management and control in high precedence levels is essential because these features can be turned against the users by taking advantage of the implicit authorities and attacking the network using its own sophistication.

A high level set of scenarios were developed for Information Assurance attacks against the GIG. These attacks will take advantage of weaknesses/holes in the architecture and capitalize on features that are designed to make a system more reliable.

- ***Malfunctions Attack*** - The first set is where a component on the GIG continues to broadcast, even though it is signaled by the network controller to stop broadcasting due to being preempted by a higher priority user. The lower priority messages will be dropped once they attempt cross the domain, but will continue to occupy bandwidth in the internal domain. This scenario will affect the network performance in cases where the network is congested especially with low priority traffic, or the offender has a somewhat higher priority ID.
- ***Transport Level DOS Attack*** - The second set is where an intentional attack against the network is attempted. The enemy would flood the network with high priority traffic to occupy and fill the available resources with traffic and prevent the coalition forces from using this resource. This can have a devastating outcome especially when all messaging (voice, video, text, other) are expected to use the same transport network. Protection of this asset is essential.
- ***Control Level DOS Attack*** - The third set is where a malicious attack is attempted against the control mechanisms of the GIG. The enemy attempts to seize control of the network by corrupting the controlling mechanisms to render the network useless or have access to the data and attempt to modify the contents of the messages.
- ***Overt Attack*** – Another attack scenario involves bombing or otherwise sabotage the network infrastructure by external means. These include bombing, disrupting power, etc.

Other attacks that can negatively affect the capabilities include information extortion, information sabotage and vandalism, theft, software attacks and others which can be accomplished via backdoor in one of the systems, spoofing, brute force or more sophisticated means. The risk mitigation process will involve smart architecture encompassing hardware, software and processes that give us the advantage in supporting the warfighter.

4 Architecture Issues

In this section, we discuss the current GIG P&P architecture. The first step of this description is a common understanding of the GIG through presenting a basic model of end-to-end infrastructure connectivity. The GIG is defined as a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel

The proposed P&P Architecture Description Framework is based on generic GIG P&P network architecture reference framework. This architecture framework merely identifies and labels a set of boxes and their locations in the context of a data service. The framework is divided into transport, control and network management levels. It provides a topographic relationship between the boxes, the levels and the end hosts.

4.1 Architecture Overview

A tiered Reference Architectural Model (RefAM) was developed for P&P capabilities in a packet based transport service, comprising a Local Tier and a Non-Local Tier. See Figure 1[1, 2, 5]. This architecture was proposed to address the requirements for military Precedence and Preemption. The Local Tier comprises those functions and mechanisms that take actions based upon information and state which is local to the mechanisms. The Non-Local Tier comprises mechanisms and functions which require coordination and information dissemination between distant components in the network. For example, a Local Tier mechanism is the service discipline implemented at the access to a network resource. A Non-Local Tier mechanism is the transmission of a resource reservation request packet from the application to the destination which establishes state at each resource along the data path and which returns information regarding the success or failure of the path to provide the requested resources. Figure 2 gives a pictorial representation of the RefAM. It shows the local functions in black and the non-local functions in blue. The letters in circles associate the various functions within the RefAM to their locations in elements comprising the transport network.

Figure 1: The Architecture Reference Framework.

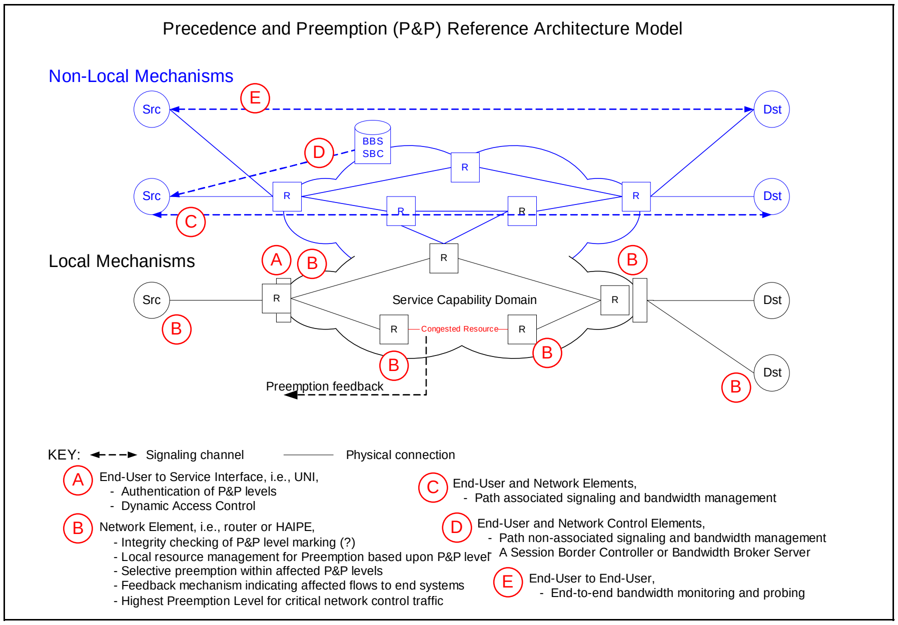
Precedence and Preemption (P&P) Reference Architecture Model
Non-Local Mechanisms
E
Src
Dst
D
BBS
SBC
R
Src
R
R
R
R
Dst
C
Local Mechanisms
A
B
R
B
Src
R
Service Capability Domain
R
Dst
B
R
Congested Resource
R
B
B
Dst
Preemption feedback
B
KEY:
Signaling channel
Physical connection
A
End-User to Service Interface, i.e., UNI,
- Authentication of P&P levels
- Dynamic Access Control
B
Network Element, i.e., router or HAIPE,
- Integrity checking of P&P level marking (?)
- Local resource management for Preemption based upon P&P level
- Selective preemption within affected P&P levels
- Feedback mechanism indicating affected flows to end systems
- Highest Preemption Level for critical network control traffic
C
End-User and Network Elements,
- Path associated signaling and bandwidth management
D
End-User and Network Control Elements,
- Path non-associated signaling and bandwidth management
A Session Border Controller or Bandwidth Broker Server
E
End-User to End-User,
- End-to-end bandwidth monitoring and probing

Figure 2: The Precedence and Preemption Reference Architectural Model

So, the proposed network architecture for P&P packet transport service, minimally consists of the following Local Tier components:

- **Authentication and Integrity Checking** - P&P capabilities allow for higher precedence messages to access the network resources in favor of lower precedence messages[2].
- **Host-based Packet Marking** - fundamentally, the GIG is a packet transport service and the base transport network takes actions, e.g., forwarding, on individual packets.
- **Local Resource Management** - some of the most effective schemes for resource management, e.g., P&P, are local management capabilities resident at the congested resource.
- **Selective Discard Mechanisms** - when packets are discarded based upon Network Precedence Level markings, the network elements should do so in the most unobtrusive way as possible.
- **Explicit Notification** - it is required that feedback be provided upstream to voice and video applications, end-users or middle boxes in the event that flows are being preempted.
- **Signaling** - The network architecture for military Precedence and Preemption additionally consists of Non-Local Tier components. Possible non-local mechanisms include:
  - Application Level Signaling
  - Path Reservation Signaling
  - Bandwidth Broker and/or Session Border Controller Reservations
  - End-to-End User Monitoring
  - Network Usage Policy
- **OAM&P** - There are no guarantees afforded to the transport of lower Network Precedence-Level packets in the presence of higher Network Precedence-Level traffic.

4.2 Access Control

P&P capabilities allow for higher precedence messages to access the network resources in favor of lower precedence messages. Hence, it is imperative that effective authentication mechanisms are part of the architecture. Authentication functions must be performed at the network service interface, i.e., the User to Network Interface (UNI), as indicated by the label Circle-A in Figure 3. The RefAM assumes that

- The network authenticates the identity of the end user.
- The network interface implements some form of packet access control which is minimally configured into the interface by a network management and provisioning function or preferably associated with the end user authentication function.
- The packet Access Control List (ACL) is based upon source and destination packet addresses. Hence, the architecture assume no capability for address spoofing between the host and the UNI.
- The ACL indicates the highest Network Precedence-Level of the packets that are allowed to enter the network over that interface, unless generated in response to outbound packets of a higher Network Precedence-Level. Hence, the access control is required to have a dynamic component, which correlates outbound NPL indications to allowed inbound NPL indications.

From an IA perspective with respect to the Access Control component of the P&P RefAM:

- The authentication mechanisms need to be defined within the P&P RefAM.
- The coordination mechanism between the authentication function and the packet level ACL at the network interface needs to be defined.

[2] We use the term Precedence-Level (PL) as the precedence level of the message as indicated by the end user or source of the message. We will refer to the Network Precedence-Level (NPL) of a packet as indicated by packet marking.

- The IA implication of supporting a multiplexed network interface and relying upon ACLs based upon the integrity of packet level addresses need investigation. At a minimum, the GIG architecture needs to insure the security of the access infrastructure delivering packets to the network level interface point.
- Finally, the security implications of relying on a dynamic ACL mechanism and the development of the algorithms for the dynamic ACLs need investigating.

4.3 Host-based Packet Marking

Fundamentally, the GIG is a packet transport service and the base transport network takes actions, e.g., forwarding, on individual packets. Hence, it is necessary to indicate on the packet the NPL associated with the end user or source message's Precedence Level. This per packet marking is required because not all communications (or messages) are session-based; often an application may generate one or a few packets. The QoS Class marking to be carried in packet headers indicates the type of application generating the transport packets. There has been discussion of the IA implications of explicitly identifying this type of information within the GIG's Black Transport Core. Given that the P&P RefAM relies upon including additional packet header tags which carry the end user Precedence Level associated with the perceived importance of the information carried within the packet, we suspect that the IA implications of this additional packet tag should be of greater concern. The NPL packet markings carry many of the same IA concerns as carrying the QoS Class packet markings. In addition, the NPL markings open up potential Denial of Service (DoS) attacks and potential traffic analysis based upon the importance of the message contents. Based upon this packet marking, more directed attacks against the GIG infrastructure may be possible and this directed attack may be harder to detect. This type of information in the packet headers needs to traverse the Red-Black interface.

4.4 Local Processing

Some of the most effective schemes for resource management, e.g., P&P, are local management capabilities resident at the congested resource. This is especially true in tactical wireless networks. Hence, the P&P RefAM provides a local resource management function. Specifically, these functions include service discipline and active queue management capabilities within the transport architecture. A novel example of this type of local processing is found and analyzed in [12]. We will refer to these mechanisms collectively as the Per Hop Behavior (PHB) mechanisms. These mechanisms should be supported in all network elements performing a statistical multiplexing function, as indicated by the label Circle-B in Figure 2. This includes hosts, routers, HAIPEs, etc. Some local processing scheduling algorithms are more susceptible to DoS attacks than other scheduling algorithms. For example, a strict priority scheduler based upon the NPL markings on the packet headers is highly susceptible to DoS attacks in the following sense. Once a higher NPL is under attack, all network access to lower NPLs is totally excluded. This may be a highly undesirable outcome. Other scheduling algorithms which ensure some lower level bandwidth access to lower NPLs, may be more resilient to DoS attack and better support network recovery from DoS attacks. The characteristics of preferred schedulers should be identified in the context of an IA analysis. Typically, HAIPEs are excluded from the discussion of desired PHB models because it is wrongly assumed that HAIPEs never get into a congested state. However, due to the transport overhead associated with data packet encryption, HAIPEs can and do get into congested states and must discard packets. Therefore, HAIPEs need to support the PHBs associated with P&P requirements.

4.5 Selective Discard Strategies

When the network is in an overloaded state, it must make hard decisions with respect to packet discarding and session level preemptions. However, for any given situation, the network is required to discard only a fraction of the traffic at a given NPL. Hence, it should have a Selective discard Strategy at hand in order to decide what flows to preempt and what traffic to allow. In a single service network, e.g., a telephony network, selective discarding degenerates simply to preempting just enough of the calls to allow the higher NP calls to complete. However, in a multi-services packet transport environment, the selective discard strategies are more complex. Selective Discarding can be viewed as a type of precedence level, only operating at a finer grain of control. Hence, if the specific selective discard algorithm or strategy is known, an attacker can use this information to perform a DoS attack in the same fashion as performing a DoS attack against the local processing component of a P&P enabled transport service. If the network is designed to allow local intent to determine the selective discard strategy through some form of network policy-based management process, then this channel may be used to affect undesirable behavior within the network. This policy-based management control process needs to be secure against intrusions.

4.6 Explicit Preemption Notifications

It is required that feedback be provided upstream to voice and video applications, end-users or middle boxes in the event that flows are being preempted. This capability is required for both soft preemption mechanisms, e.g., packet discard, and hard preemption mechanisms. The form of the notifications for soft and hard preemption will be different. However, a form of explicit notification is included at all network elements performing a statistical multiplexing function, as indicated by the label Circle-B in Figure 2. For soft preemption, the selective discard mechanism identifies a subset of the flows on which to implement preemption, i.e., packet discard, it must maintain a memory related to the selected flows and send notifications back up stream toward the source of the packet flows suffering preemption [7]. It is not necessary that notifications are sent for every dropped packet, but only occasionally for sessions being preempted. These notifications will carry the P&P NPL markings and be sent to the address of the application source. The algorithm for tagging packets with an explicit notification is currently is the subject of another research effort. However, the contents and form of the notification messages have been analyzed within the context of various analysis/deployment models in for IPv4 technologies, for IPv6 technologies and [4] for MPLS technologies. It is left to the application, middle boxes, or other elements in the overall service architecture to take actions based upon these soft preemption notifications. The existence of Preemption Notification opens the door to spoofing of the notifications leading to DoS attacks. This holds for both soft preemption, relying upon ICMP messages for notification, and for hard preemption, relying upon RSVP messages for notification. This type of notification needs to traverse the Red-Black interface.

4.7 Signaling

The P&P RefAM consists of Non-Local Tier components. Not all non-local components are necessary, but some form of non-local mechanisms are required to fully meet the requirements and goals. Possible non-local mechanisms include:

- **Application Level Signaling** - it is desirable for the application to be able to indicate, through some form of signaling, their minimum desired Quality of Service (QoS) requirements and associated Precedence Level. This allows the transport service to be able to more intelligently coordinate and determine when Preemption conditions exist and how to coordinate Preemption to optimize network-wide performance.
- **User to Edge Signaling** - the application needs to be able to indicate, through some form of signaling, their minimum desired QoS requirements and associated Precedence Level. One option is to support an application to network interface signaling method. The network may use this information to configure rate filters at the UNI for that flow.
- **Path Reservation Signaling** - the network may choose to pass application level signaling information along the desired router path across the network and to allow the component along the path to build state to enhance overall network performance and handling of Preemption events. An example of this type of signaling would be end-to-end, path associated RSVP signaling.
- **Bandwidth Broker and/or Session Border Controller Reservations** - the network may choose to pass application level signaling information to a centralized Bandwidth Broker Service (BBS) or an edge based

Session Border Controller (SBC) which would be responsible for reserving the appropriate state information along the desired routed path to enhance overall network performance and handling of Preemption events. A related option is a gateway device, e.g., the U.S. Army's QED which passively monitors portion of the GIG which it cannot view explicitly and make appropriate preemption decisions based upon its passive results.

- **End-to-End User Monitoring** – some end-to-end protocol incorporate channel monitoring in order to decide how to optimize performance. An example of this is the monitoring reported within an RTCP channel. Other methods are possible, e.g., the packet time stamping implemented in the U.S. Army's development of the QED gateway device
- **Network Usage Policy** - it is necessary to understand the limitations of the deployed architecture for P&P services and to employ forms of Correct Usage Policy to ensure correct functioning of the network.

The presence of a signaling protocol opens the door for spoofing of messages resulting in DoS attacks, as previously discussed in the context of Explicit Preemption Notification messaging. The vulnerabilities inherent in the chosen signaling protocols, e.g., RSVP and SIP, needs analysis. An example is a DoS attack based upon overloading the networking infrastructure with high volumes of setup and teardown requests. Additionally, the IA impact of passing this signaling information over the Red-Black interface needs analysis.

4.8 Network OAM&P

DoD style P&P is often referred to as ruthless. There is no guarantee afforded to the transport of lower Network Precedence-Level packets in the presence of higher Network Precedence-Level traffic. Thus, it is necessary that a highest Network Precedence-Level be identified, above all end user indications of Precedence-Level, for the sole purpose of carrying only network critical control traffic. This is traffic which supports the basic connectivity requirements of the network. Use case analysis has determined what control traffic is considered appropriate for inclusion into this Critical Network Control (CNC) Network Precedence-Level. The OAM&P architecture associated with P&P packet transport services is yet to be defined. Within the context of IA analysis, consideration of the appropriate monitoring, intrusion detection, header modification detection and fault isolation capabilities need definition. These mechanisms need to ensure that the network will perform correctly in the presence of a set of well defined Attack Scenarios. The objective of the CNC PL is to keep the network functioning while not overloading the CNC NPL with unnecessary traffic. Further, no end user traffic should be capable of accessing the CNC NPL. This implies restrictions on the authentication and access control functions at the network interface, i.e., end users should not be receiving CNC traffic so the dynamic access control should never allow an end user to send CNC traffic into the network.

5 Conclusion

The success of the GIG will depend in large part on how well it helps achieve fully interoperable forces by connecting today's islands of interoperability to allow force-wide information sharing. In the context of telephony, the precedence level is set or assigned by the calling party at the beginning of a call, on a per call basis. This analysis centered on how to best architect and support data communications services through P&P capabilities while at the same time providing for Information Assurance. For the GIG, being an IP-based environment, this analysis considered the architectural aspects for access control, host-based packet marking, local processing, selective discard strategies, explicit preemption notifications, signaling and network OAM&P and made recommendations for IA implications. The analysis is by no means complete, but is a first step into determining the essential IA requirements that are associated with the P&P on the GIG to ensure that the Precedence services will enhance the GIG and allow the users to efficiently utilize the scarce resources in the best possible manner and reduce the intentional abuse or unintentional faults. The next step is to choose the critical requirements and specify specific algorithms necessary to complete a full description of the P&P reference architecture. This include algorithms for dynamic access control, per packet integrity checks, selective discarding and preemption notifications, per hop behaviors and reservation algorithms tied to the non-local components of the architecture. As these algorithms gain specificity, it will be necessary to run the simulations to validate their expected characteristics as measured against the critical requirements. Much work remains in the area of requirements analysis and architecture development in this important field of packet based data networking.

6 References

[1] Requirements and Architectural Analysis for Precedence Capabilities in the Global Information Grid; B. Farroha, A. DeSimone, B. Liebowitz. MILCOM 2006

[2] A Hybrid End-to-End QOS Architecture for Heterogeneous Networks (like the Global Information Grid) Bharat Doshi, Lotfi Benmohamed, Antonio DeSimone; MILCOM 2005

[3] Chairman of the Joint Chiefs of Staff – Instructions (CJCSI), "Policy for Department of Defense Voice Networks", CJCSI 6215.01B, 23 September 2001.

[4] Precedence and Quality Of Service (QOS) Handling in IP Packet Networks; D Goldsmith, B Liebowitz, K Park, S Wang, B Doshi, J Kantonides. MILCOM 2006.

[5] "End-to-End QoS Over the GIG, Bharat Doshi, Lotfi Benmohamed, Antonio DeSimone, Kenneth Schmidt, MILCOM'04.

[6] DoD Instruction (DODI) 8100.3, "Department of Defense (DoD) Voice Networks", 16 January 2004

[7] ITU (CCITT) Recommendation I.255.3, Multilevel Precedence and Preemption Services (MLPP).

[8] Mission Area Initial Capabilities Document (MA ICD), Global Information Grid (GIG), JROCM 202-02, 22 November 2002

[9] DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy", September 19, 2002

[10] IETF Draft, "Configuration Guidelines for DiffServ Service Classes", draft-baker-diffserv-basicclasses-04.

[11] ITU Recommendation Y.1541, "Network Performance Objectives for IP-Based Services", 2003.

[12] Cole, R.G. And P. Chimento, "Modeling and Preliminary Simulation Studies for Packet Based Precedence and Preemption for FCS Communications", Army Science Conference 2006, Orlando, FL, USA, December, 2006.