

Global Secure Communications: Challenges and Opportunities

Bharat T. Doshi

Experiences from recent wars against nations and global terrorism have identified a need for a much higher degree of information sharing and joint decision making among various intelligence agencies, different armed forces, and the central command and control structure. Meeting this need calls for an orders-of-magnitude increase in computing and communications capacities and replacement of current stove-piped information systems and networks by an integrated infrastructure and service creation environment for the DoD, intelligence, and homeland security communities. Based on the tremendous success of the Internet and web in providing an integrated environment and productivity gain in the commercial arena, the U.S. government has embarked on an ambitious journey toward creating the Global Information Grid (GIG) to enable net-centric operations and warfare. Indeed, Internet, web, and several related technologies, having provided major drivers for recent commercial successes, are ideally suited to move toward the realization of the GIG vision. However, a number of technical challenges need to be addressed. APL is contributing to this effort and should continue to play a major role in helping the government and industry create technical solutions to these challenges. This article highlights some of these challenges and discusses advanced work to which APL can contribute.

INTRODUCTION

The 20th century and early 21st century have brought major advances in computing and communications technologies. These advances have changed the way we work and live and have also become new weapons for business and national superiority.

Basic telephony began to penetrate the market in the early part of the 20th century. In the second and third quarters of that century, basic telephony became an immense global capability for instantaneous two-way

communications. A combination of copper loop, coaxial cable, microwave, fiber, and satellite systems provided media for high communication capacity in dense urban areas while also enabling connectivity to remote locations around the globe. During the last quarter of the 20th century and the beginning of the 21st century, technology advances, regulatory changes, and competition have made basic telephony cheaper and increasingly accessible. Advances included digitization of the

earlier analog infrastructure, the ever-widening capacity of optical fiber along with decreasing unit cost, and the addition of service intelligence. The infrastructure created to provide telephony service was an engineering marvel that also allowed private line services to enterprises for creating their own services over raw communications capability.

While wireless access technologies were applied first in military communications and in special commercial sectors (e.g., truckers, police, and other emergency response organizations), cellular systems have taken wireless communications to another dimension. In a span of less than 25 years, the number of cellular users has approached 1 billion. The ability to communicate on the move and to deploy new infrastructure rapidly has changed the telephony paradigm completely. It has created a culture of road warriors and 24/7 workers. It has also allowed countries lagging in wireline telephony to jump-start their population toward modern telephony with the rapid deployment of a wireless infrastructure.

Specialized forms of wireless communications using low-orbit or geosynchronous satellites have allowed, albeit expensively, communication from and to ships, planes, and other platforms not easily accessible via a wireline infrastructure. There is an ongoing effort in the commercial world to make this type of communication cheaper and more accessible.

Military communication has benefited tremendously from the development of commercial telephony. In fact, the government used the commercial infrastructure for most of its voice telephony needs in wireline scenarios. Some of DoD's voice communication uses a secure derivative of commercial technologies. At the same time, special geographical environments have required more wireless and satellite access for communication in the tactical battlefield and between the battlefield and the strategic backbone (reach-back). These requirements are not met easily by commercially available technologies. Thus, the DoD has created many innovative telephony systems using ground-, sea-, air-, and space-based wireless access technologies. Also, novel techniques have been developed to keep communications secure and circumvent hostile weather and/or adversarial jamming. However, low information rates and hostile RF environments have required that tactical users accept significantly worse voice quality than commercial telephony users. In addition, the large propagation delays over satellite links created an almost half-duplex telephony service that tactical military users became used to.

While wireline and wireless telephony were major forces shaping 20th century commercial operations, telephony is point-to-point (or multipoint-to-multipoint in a telephone conference) planned communication. Users had to know with whom they wanted to communicate, phone numbers to be reached, etc. The advent of data networking in the last quarter of the last century

allowed communication and information sharing without the need for the parties to interact directly.

A number of different technologies have been developed and used to provide data networking capability. Among them are DECnet, SNA, X.25, Frame Relay, ATM, IP, and Ethernet. (As the use of the acronyms in this article is widespread, the boxed insert lists their meanings for those readers unfamiliar with the terminology.) The combination of IP and Ethernet has become the dominant workhorse of data networking today, especially among ISPs. However, Frame Relay and ATM continue to play significant roles in wide-area networking services provided to enterprises by large commercial carriers. Most data end systems use IP and Ethernet. Frame Relay and ATM, where used, encapsulate IP-based datagrams and carry them in tunnels called "virtual circuits." Besides providing connections in the form of virtual circuits, Frame Relay and ATM also provide traffic engineering, service-level guarantees, better management of failures, and routing controls. MPLS has recently been used to provide these capabilities in IP networks.

Many of the early applications of data networking required data generators to know the data users and vice versa. However, the Internet/web combination thoroughly exploited the ability to separate the producer and consumer of the data. Both the public Internet and private Enterprise intranets using web-based services allow anyone to create and post information and to search for and retrieve that information without even knowing its source. This has created a major revolution in information sharing. It has also generated tremendous productivity gains, information superiority, and competitiveness.

Finally, the Internet and web have changed the way we shop, study, and entertain ourselves. IP-based networks have even started offering voice telephony services. Distributed controls, universal interoperability, unlimited scalability, and rapid service creation have allowed the IP-based Internet and intranets to sustain rapid growth and an unprecedented rate of introduction of new services.

Whereas early commercial wireless systems were focused on voice telephony, second-generation cellular systems allowed short message services that became very popular as a means of communication. Later technologies have provided the ability to receive e-mails, images, and even video over cellular systems. On the other hand, the recent proliferation of IEEE 802.xx-based wireless LANs has enabled the creation of hot spots where the users can get megabits-per-second connectivity. These data services use IP-based protocols and are readily interoperable with the IP services available on wireline access networks.

Thus, the commercial world has seen the explosion of the Internet and intranet to supplement ubiquitous

ACRONYMS

AAA	Authentication, Authorization, and Accounting	MAC	Medium Access Control
AAV	Advanced Aerial Vehicle	MANET	Mobile ad hoc Networks
ADNS	Advanced Data Network Solutions	MIMO	Multiple In, Multiple Out
AoA	Analysis of Alternatives	MPLS	Multi Protocol Label Switching
ATM	Asynchronous Transfer Mode	MUOS	Mobile User Objective System
BGP	Border Gateway Protocol	NCES	Net Centric Enterprise Services
C2	Command and Control	OSPF	Open Shortest Path First
CT	Cloud Type	PBNM	Policy Based Network Management
DiffServe	Differentiated Services	PT	Packet Terminal
DISN	Defense Information Systems Network	QoP	Quality of Protection
FCAPS	Fault, Configuration, Accounting, Performance, and Security	QoS	Quality of Service
FCS	Frame Check Sequence	R-SLC	Routing-Service Level Capability
GEOS	Geosynchronous Earth Orbiting Satellite	RSVP	Resource ReSerVation Protocol
GES	GIG Enterprise Service	RTP	Rapid Transport Protocol
GIG	Global Information Grid	SCA	Software Communications Architecture
GIG-BE	GIG-Bandwidth Enhanced	SCD	Service Capability Domain
GW	Gateway	SIP	Session Initiation Protocol
IA	Information Assurance	SLA	Service Level Agreement
IEEE	Institute of Electrical and Electronics Engineers	SLC	Service Level Capability
IETF	Internet Engineering Task Force	SNA	Systems Network Architecture
IntServe	Integrated Services	TCP	Transmission Control Protocol
IP	Internet Protocol	TCS	Tactical Control System
IPSEC	IP SECurity	TDC	Tabular Data Control
IS-IS	Intermediate System-Intermediate System	TPED	Task/Process/Exploit/Disseminate
ISP	Internet Service Provider	TPPU	Task/Post/Process/Use
ITU	International Telecommunication Union	TSAT	Transformational SATellite System
JTF-GNO	Joint Task Force-Global Network Operations	UAV	Unmanned Aerial Vehicle
JTRS	Joint Tactical Radio Systems	UDP	User Datagram Protocol
LAN	Local Area Network	UGS	Unattended Ground Sensor
LEOS	Low Earth Orbiting Satellite	VPN	Virtual Private Network
		WGS	Wideband Gap Filter System
		WIN-T	Warfighter Information Network-Tactical
		WNW	Wideband Network Waveform

telephony services as well as a major explosion in wireless telephony. We are now also looking at the beginnings of the convergence of voice, data, and video services on both wired and wireless networks.

The DoD and intelligence communities have not benefited fully from these advances, from infrastructure integration, or from the new information sharing paradigm. Although they do use many of the technologies and protocols that are creating the revolution in the commercial world, their networks and information systems are stovepiped and have little interoperability. There are also critical bottlenecks in tactical networks,¹ and the information sharing philosophy is based on “need to know” rather than “need to share.”

Experiences during recent wars against nations and global terrorism have shown that the ability to receive superior intelligence from multiple sources and media, to move information rapidly, and to carry out joint missions easily has had a major force multiplier effect. However, as mentioned above, these capabilities do not exist ubiquitously, and experiences have also exposed vulnerability caused by bandwidth bottleneck and stovepiped communication infrastructure.

These experiences and the success of the Internet in the commercial world have prompted the government to embark on an ambitious undertaking to build an integrated infrastructure for all DoD and intelligence communities. This infrastructure may eventually integrate the one being built for homeland security, law enforcement, and other civilian functions. This major undertaking is accompanied by a fundamental shift in the philosophy of information sharing; i.e., the TPED (Task/Process/Exploit/Disseminate) philosophy is replaced by the TPPU (Task/Post/Process/Use) philosophy² that has transformed Enterprise data dissemination in the commercial arena. TPED implies that the collector of information will send it to processing entities that will process and filter the information, decide who may benefit from it, and send it to those identified as beneficiaries, if the policies allow those people access. This process is slow, and many potential beneficiaries may not be identified and thus never receive information valuable for their mission. The TPPU philosophy, on the other hand, will make raw information available to all as soon as it is collected. People who are entitled to look at the information can use intelligent pull technology as soon

as the information is posted. TPPU is not unlike the way we use Internet and web searches today.

Collectively, the integrated infrastructure and uniform service creation environment is called the Global Information Grid (GIG).

THE GIG VISION AND NETWORK INFRASTRUCTURE

The GIG vision involves an integrated information systems infrastructure, a network infrastructure, services platforms, and an applications environment that allow the TPPU philosophy to be deployed for the entire user community. Underlying the GIG vision is a global network infrastructure that is based on a few key tenets³:

- IP as a common network layer protocol throughout the GIG so networks using various physical and link layer technologies can interoperate at network and higher layers
- Standards-based intra- and inter-domain routing protocols (e.g., OSPF, IS-IS, BGP, etc.)
- Standards-based higher-layer protocols (TCP, UDP, http, RTP)
- Protection of the use traffic by encrypting as close to the source end device as possible and then decrypting as close to the destination end device as possible
- The cyphertext core as a single contiguous black core
- High-capacity optical backbone where possible
- High-capacity satellite communications using routers in satellite platforms and cross-links
- A family of software radios (JTRS) with a common software communications architecture (SCA) providing the foundation for tactical wireless communications on the ground, at sea, in the air, and in space
- Standards-based MANETs to create wireless network infrastructure using JTRS
- Migration of all communications services/applications to the new IP-based infrastructure

The focus of this article is on the network infrastructure as listed below. However, we do list similar tenets for information systems infrastructure and services platforms.

- Web services providing the foundation for a service creation environment
- A set of core services under the umbrella of NCES; warfighter,

business, and C2 applications over these common sets of core services

- An information assurance (IA) architecture that is integrated into the overall GIG architecture, allowing TPPU while strengthening IA and being as unobtrusive as possible

Figure 1 shows the overall GIG architectural decomposition. Figure 2 illustrates the transport network infrastructure envisioned for the GIG. This network infrastructure comprises³⁻⁶

- JTRS-based MANETs in tactical networks on the ground, at sea, and in the air
- Tactical deployed networks such as FCS, WIN-T, ADNS, and TDC
- Satellite systems such as MUOS, WGS, and TSAT
- High-capacity IP-optical backbone in the form of GIG-BE to be integrated into the next-generation DISN IP core
- Teleport providing connectivity between deployed satellite systems and fixed backbone

The GIG will also interface with many existing legacy systems and their evolutionary replacements.

As mentioned earlier, the current infrastructure used by the DoD and intelligence communities involves many individual networks and information systems with little interoperability. Communications between lower echelons of two different services may involve several levels of hierarchy. Joint operations are difficult and cumbersome. Intelligence is fragmented. Much of the infrastructure uses a circuit approach and takes a long time to provision. Communications support for important missions may take months of planning and provisioning. And replanning for changes in a mission may take days or weeks.

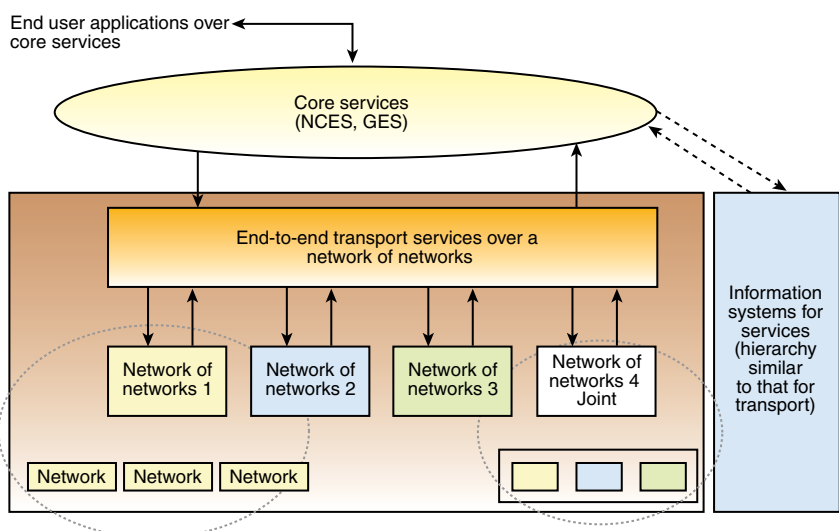


Figure 1. Client server architecture for services (e.g., warfighter and business applications) over a common shared infrastructure.

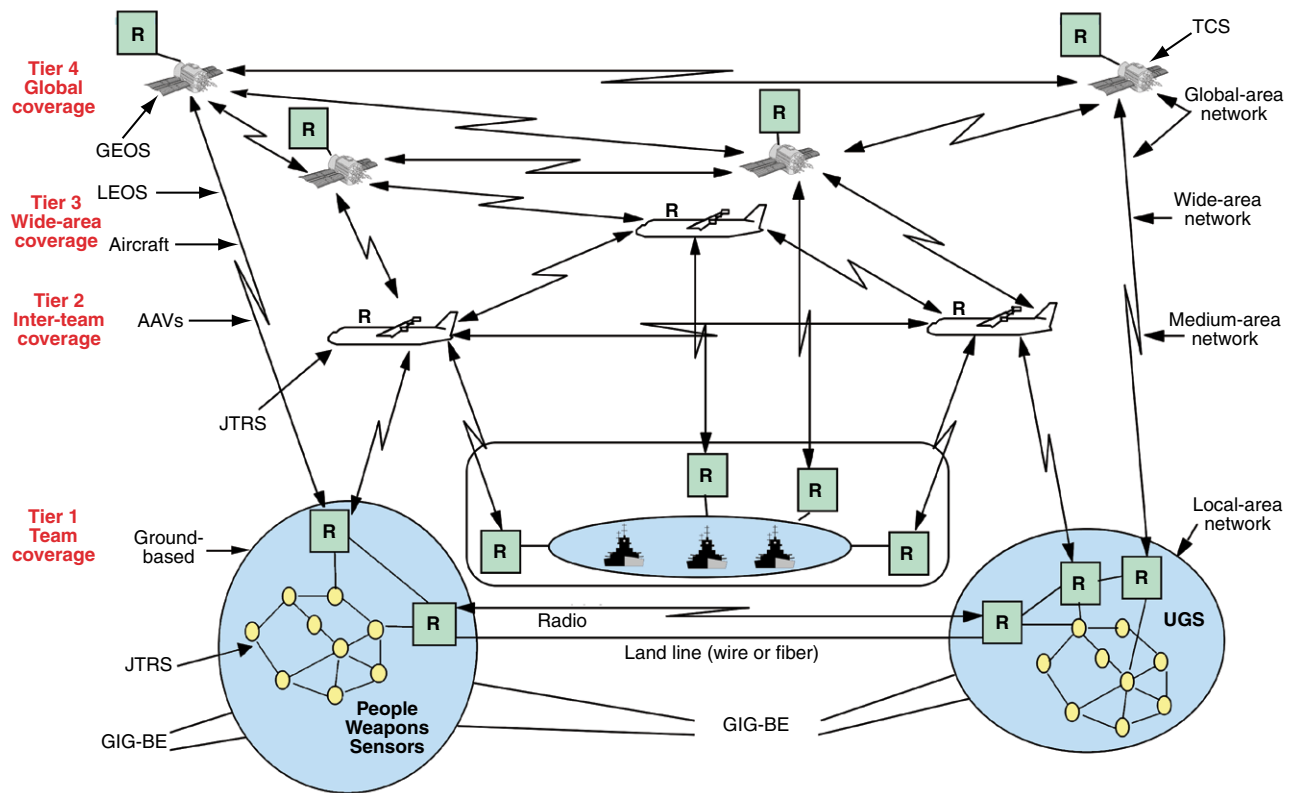


Figure 2. The GIG transport infrastructure ("R" = Internet router).

Technologies proposed for the GIG network infrastructure make it much more dynamic. In particular, distributed controls, distributed routing decisions, self-healing by rerouting after failure, and statistical multiplexing allow the network to be efficient, interoperable, and reconfigurable to meet changing needs. Also, some of the technologies (e.g., optical) provide a tremendous increase in bandwidth at a reasonable cost. Similar changes are possible for the information systems infrastructure. Thus, a successful deployment of the net-centric GIG can bring many advantages to the DoD and intelligence communities:

- Major reduction in communications planning and deployment time for major missions
- Flexibility to create short-term mission support in hours and replan in minutes
- Global connectivity and communications on demand, sometimes using specialized communications relays (ground-, sea-, and air-based) for added connectivity
- Tremendous increase in bandwidth availability, even to the tactical battlefield, making it possible to use richer media (images, video), provide better intelligence to and from the battlefield, and allow a high degree of horizontal communication
- Total situation awareness from the fusion of multiple types of sensor data
- Innovative sensor-fusion-action capabilities
- C2 based on near-real-time information
- Decentralization of decisions and actions: top commanders communicating intent based on mission needs and intent executed by local commanders based on a richer set of local information
- Increasing ability to carry out joint operations
- Extraordinary ability to fuse strategic intelligence from multiple sources (human, voice communication, e-mails, images, video, etc.) to provide superior intelligence about nation states as well as terrorist organizations

As noted above, experiences have shown the force multiplier effect of such superior situation awareness, rapid mission planning and replanning, distributed intelligence, and distributed C2. The GIG vision is to provide an asymmetric advantage in the information plane, similar to that enjoyed by the United States in the kinetic battlefield, to maximize the force multiplier effect and change the basic nature of warfare. In effect, the GIG vision is to enable a major force transformation. Homeland security, emergency response organizations, and law enforcement agencies can benefit from the information superiority that the GIG-type integrated architecture can provide. Equally important, giving these organizations the information infrastructure that can interoperate with the DoD and intelligence communities' infrastructure will be critical to the future success of all.

A key aspect of the GIG vision is that it is based on commercial technologies and standards. On one hand, this approach allows the government to benefit from significant advances over the last two decades in the networking industry. It also reduces the cost structure. Finally, it allows continuing technology refresh and makes the GIG future proof. However, realizing the GIG vision is not trivial. While commercial technologies and experiences will be useful, many technical challenges still need to be addressed. These challenges are in both the computing and communications infrastructure and end-to-end operations. In this article, our focus is on the communications and networking aspect of the GIG.

CHALLENGES

Challenges arise from several dimensions in which the GIG differs from the successful commercial Internet and intranets:

- A much stronger focus on the mission and more dynamic missions
- More demanding and more diverse requirements from applications
- New requirements on relative precedence based on user and mission identities (e.g., multi-level priority and precedence used in circuit-based voice telephony today)
- The much higher importance of security in military communication
- A much higher fraction of users with wireless access
- The significantly higher use of satellite communication and the first use of satellites with routers onboard
- More widely varying (spatially and temporally) RF conditions, which make the basic resource itself unpredictable
- A much larger fraction of communication over mobile ad hoc networks, which have not matured in commercial networking
- A much higher degree of infrastructure mobility (a few miles per hour at sea to a few tens of miles per hour on the ground to a few thousand miles per hour in the air) in addition to user mobility
- An operational model that has elements of the public Internet as well as those of a large Enterprise intranet

In the following sections we translate some of the above challenges into specific problems to be solved. We focus on those problems that APL can and should help solve.

Removing Bandwidth Bottlenecks

The GIG comprises a very diverse set of networks. We have defined^{7,8} an SCD to be a relatively

homogeneous and connected network with well-defined interfaces and gateways to the rest of the GIG. Thus, each SCD should have one physical-layer and one link-layer technology. It should also have a uniform set of mechanisms to provide relative and absolute QoS capabilities. A typical autonomous system in an IP federation of networks may have one or more SCDs or vice versa. Having multiple SCDs per autonomous system is the more likely scenario.

SCDs vary widely in their data rates. Some, such as the IP/Optical backbone, can deliver enormous data rates very inexpensively owing to the tremendous commercial investment and technical advances in optical communications between 1990 and 2000. The same cannot be said about SCDs providing communication to tactical deployed forces. Even on sunny days, SCDs representing mobile ad hoc networking pose a bandwidth challenge. The data rate is even lower when faced with hostile weather, jamming, terrain-based fading, etc. Frequently, a MANET may have many dynamic SCDs with very different characteristics and data rates that change with time. Some satellite-based SCDs have similar problems with dynamic resource capacities.

While the commercial world has seen major improvements in data rates available from cellular wireless systems and wireless LANs, investments in improving satellite communications and MANETs in a hostile RF environment are still needed. The success of the GIG depends on getting significantly more spectrum, getting more efficient use of the spectrum, and retaining a large fraction of this data rate when faced with jamming and weather-related impairment. Equally important is the need to support connectivity at a high data rate when the user terminal is on the move. The GIG needs this for ground-, sea-, air-, and space-based networking.

Although some of these challenges are similar to those encountered in commercial cellular and wireless LAN systems, additional challenges are posed by military-unique environments and requirements. The challenges also depend on whether the platforms are ground-, sea-, air-, or space-based.

To solve these challenges, APL has the right experience and expertise to help in many ways.

- Bringing expertise in propagation modeling, RF link analysis, military satellite communications, MIMO systems, and cognitive methods applied to RF communications to help design spectrum-efficient waveforms and systems and to make the systems self-learning and hence even more spectrum-efficient
- Harvesting spectra in newly opened ranges by overcoming technical obstacles in those frequency ranges
- Designing spectrum-agile protocols to allow efficient and flexible system design

- Creating solutions where intelligent local routing and recovery can be employed to use the spectrum most efficiently, even when some links have poor RF characteristics. Given the possibility of inexpensive, multirate, and multichannel radios, it will be possible to deploy a dense grid of radios, and this ability to use higher-layer intelligence to overcome problems at the physical layer will become extremely useful in creating high-capacity and reliable mobile networks.
- Bringing the expertise above to help the DoD and intelligence communities evaluate alternatives and recommend the best solution among those offered
- Incorporating the above solutions in end-to-end networking problems as described below

These challenges are important opportunities for APL. Recent involvement with several AoA projects with DoD and in internal research and development projects^{9,10} provide the right starting points to launch major initiatives. The solutions will involve innovations at many layers of protocol stacks as well as cross-layer innovations. In addition, APL has been contributing to solving communications problems related to distributed sensor fields,^{11,12} an area of critical importance and opportunity, given the advent of low-cost, low-power sensing and communications devices and the need created by asymmetric threats from hard-to-track adversary objects (e.g., submarines).

Enabling End-to-End QoS over GIG Transport

Recall that we defined the concept of SCD to simplify and scale management and controls. In practice, SCDs may be organized hierarchically so that each SCD is relatively homogeneous while significant differences are possible among them, even at the same level of hierarchy. Intra-SCD controls are decoupled from inter-SCD controls. Another concept we introduced is that of QoS in a broad sense, which includes packet-level QoS metrics such as delay, jitter, loss ratios, and data rate. These are the metrics on which the IETF has focused most effort. APL's Broad Sense QoS also includes important connection-level metrics such as "session set-up time," "time to change waveform," "time to authenticate user," etc.; security metrics such as integrity, confidentiality, availability, and quality of protection (QoP); and management plane metrics such as "time to add capacity" and "time to recover from failure." Bounds on acceptable values of the QoS metrics are called QoS requirements. The values of QoS metrics possible between edges of an SCD are called service-level capabilities of that SCD (SCD-SLC), another concept we introduced.^{7,8} The values of metrics possible over a route through GIG SCDs are called route SLCs or R-SLCs. The diversity of QoS requirements and the diversity and dynamics of SCDs (and hence variations in SCD-SLCs) making up

the GIG transport generate another set of challenges not adequately addressed by the public Internet and even by the most advanced enterprises and common carriers.

A number of standards have been developed by the IETF, ITU, IEEE, and other committees to allow the creation of solutions that support some aspects of the Broad Sense QoS we described. Among these are Diff-Serve; IntServe; RSVP; Bandwidth Brokers; traffic engineering extensions of DiffServe, OSPF, MPLS, and RSVP; extensions of SIP and H.323; the QoS-aware MAC layer in MANET; and Fast Reroute in MPLS networks. Most of these pertain to controlling the packet delay, losses, and jitter. In addition, IPSEC and AAA protocols are used to enable security features.

These standards, by themselves, do not create the needed solution. Moreover, commercial deployment of even this limited suite is meager. Thus, while the lessons learned from limited deployment will be useful in creating solutions for the GIG, we do not have solutions ready to meet the needs. Clearly, enhancements of existing standards and development of new standards will be needed to address the GIG requirements adequately. Also, the standards and available technologies will need to be used innovatively to create end-to-end QoS solutions for the GIG. In particular, providing QoS requirements in an environment with a highly mobile and dynamic infrastructure with time-varying capacity is a new problem. Providing the ability to have user- and mission-based precedence and possible preemption is another requirement that commercial IP networks have not dealt with. Having requirements that change based on the mission and short-term communications needs created by new missions and mission replans are more of a rule in DoD and intelligence community networks, but exceptions in the commercial Internet. Finally, the security requirements interfere more strongly with QoS requirements in DoD and intelligence community networks than in commercial networks.

APL has an in-depth understanding of demanding warfighter applications and also has staff members with extensive hands-on experience and research contributions to the QoS mechanism in the Frame Relay, ATM, IP, and MPLS networks in the commercial arena. This combination of application knowledge and research in QoS technologies has already begun to bear fruit. In particular, APL researchers have developed new concepts like the Broad Sense QoS, SCDs, SCD-SLCs, and R-SLCs, and have articulated their use in providing end-to-end QoS effectively.^{7,8} This work needs to be taken to the next levels of detail and used to help DoD provide total QoS solutions in a network of very diverse networks supporting a very diverse set of applications. One key to providing a scalable and flexible solution is to allow individual SCDs to have their own QoS mechanisms while requiring a set of well-defined SCD edge-to-edge behaviors. APL has made great progress in helping to define

the end-to-end and SCD edge-to-edge solutions. While this effort should be continued to conclusion, APL can further help individual SCDs create internal solutions ideally suited for the physical and link technologies within the SCDs and the mobility environments in which they operate. Particular challenges are for SCDs representing ground-, air-, and sea-based MANETs. QoS in these dynamic resource environments requires innovative approaches to session and packet controls as well as to the triage order when all QoS requirements cannot be met.

On another note, scalability requires that the GIG use distributed controls and management. At the same time, GIG users will expect end-to-end service commensurate with applications and mission requirements. Service Level Agreements (SLAs) provide the bridge between the two. SLAs between a representative of each SCD operator and a representative of the user community allow the SCD operator to provide SCD edge-to-edge service-level assurance while having complete control of intra-SCD controls. Defining end-to-end requirements and allocating the requirements among SCDs are challenges related to QoS. Particularly challenging are SCDs representing MANETs and satellite networks.

APL is well poised to help address the above challenges, summarized as “having superior QoS capabilities while maintaining IA.”

Enhancing Routing and Relationships with QoS, Mobility, and Security

It is known that the traditional routing protocols in the Internet have a very limited ability to support traffic engineering, differential QoS, load balancing, and fast mobility. While intra-domain routing protocol standards have been enhanced to support traffic engineering, the ubiquitous inter-domain protocol (eBGP) still remains a simple path vector protocol providing only one route from any node to any other node. The eBGP can be enhanced to support QoS routing with one QoS metric, but QoS routing with multiple QoS metrics (different for different applications) will require a significant departure from the current BGP. In particular, multitopology (multiroute) enhancement of the BGP will be needed to support the application diversity in the GIG. Recent ongoing work at APL^{13,14} is a step in the right direction. Simultaneously, APL staff are helping the GIG systems engineering working groups to define the enhancements needed to the eBGP and recommending solution approaches.

Most of the configuration of the eBGP remains manual, and convergence time after a change in inter-domain topology may take tens of minutes to hours. This would limit the ability to handle mobile forces and changing inter-domain topologies. With the ad hoc formation of new SCDs, changing points of attachments of existing SCDs, and rapid changes in connectivity, it is critical that the routing protocols be very responsive to the dynamics. APL has just begun to address the challenge of making the eBGP capable of supporting fast and slow mobility on networks. Similarly, mobility within a domain and within SCDs needs to be addressed in a scalable manner.

In the GIG environment, security considerations add new requirements on routing protocols. In particular, one must be able to authenticate route advertisements and protect against node spoofing, node compromises, etc. Finally, the need to encrypt user data as well as original IP headers, and the desire to limit the information passing from plain text to cipher text and cipher text to plain text, create major new challenges in designing efficient routing protocols for the GIG. Many members of the APL professional staff have been working to help address these challenges. The general approach used by commercial enterprises is to create VPNs over the common infrastructure provided by the Internet. The approach proposed for the GIG is based on this secure VPN concept (Fig. 3). However, the large size of the GIG compared to that of commercial enterprises implies the need to replace the manual configuration of IPSEC gateways with automated discovery protocols in the high-assurance version to be used in the GIG. The GIG environment also needs higher diversity and survivability than commercial counterparts and thus creates challenges resulting from multihoming. APL has begun an extensive independent research and development effort

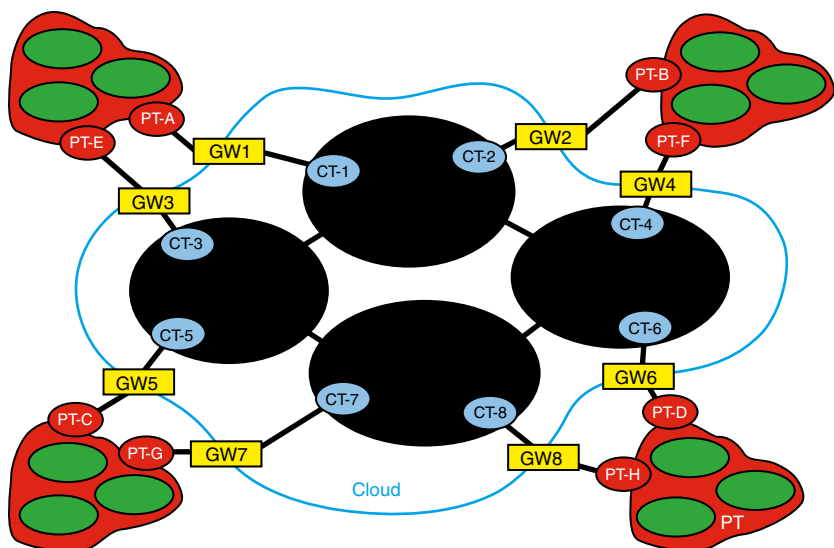


Figure 3. Secure VPNs over a single contiguous black core.

to address these problems while helping the GIG routing working group create a framework that will accept the solutions. Initial efforts by APL staff members have led to very promising solutions.¹⁵⁻¹⁷

Another routing issue involving security is the QoP concept. APL has begun an in-depth investigation of this issue in the context of inter-domain routing. The concepts of SCDs, SCD-SLCs, and R-SLCs are very useful in developing routing strategies, protocols, and algorithms involving QoP along with several other QoS metrics.

Scaling Network Management

Network management is another major challenge faced by GIG systems engineers and designers. The current Internet comprises hundreds of thousands of loosely related network domains (autonomous systems) administered and managed by separate network operators. Protocols are heavily distributed and the management plane, even within a domain, is thin compared to that in telecommunication networks supporting circuit voice and private line services. Little inter-domain management system coordination exists today, and the entire system is operated as a federated system.

Recently, there has been work on policy-based network management (PBNM) to allow network management without a central decision maker in every decision. As shown in Fig. 4a, a policy corresponds to a set of rules that suggest actions based on local observations. The decision makers create high-level policies, which can then be implemented in distributed fashion. The work is still in its infancy. Little has been done on PBNM for multiple domains arranged in flat or hierarchical fashion. Concepts of operation require a hierarchy in a multi-domain decision tree. APL has taken the initiative to extend the concept of PBNM to a multi-domain network of networks with a mix of hierarchical and flat arrangements. Policies themselves are arranged hierarchically so the highest-level policies can be

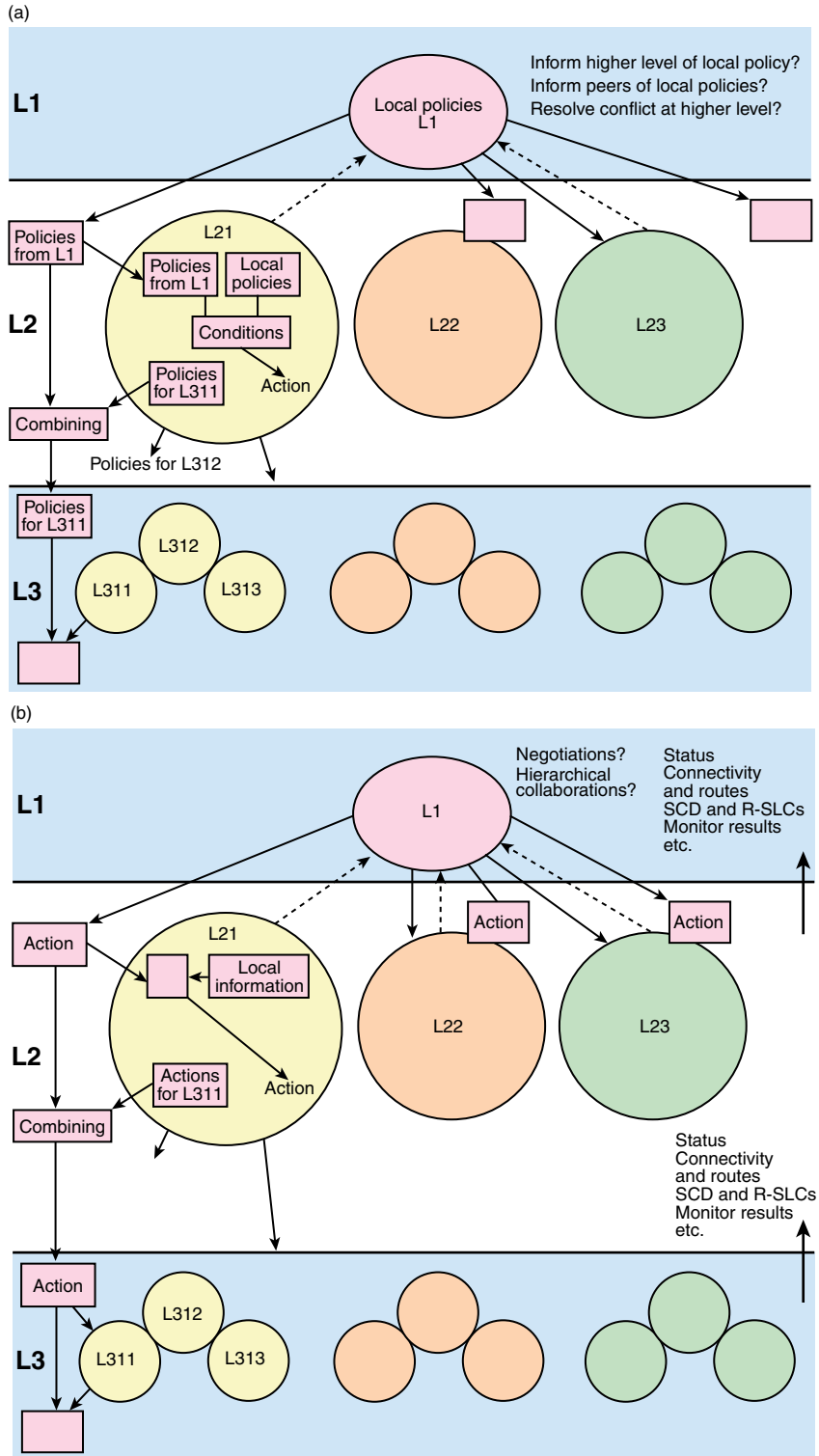


Figure 4. PBNM: (a) hierarchical, collaborative and (b) hierarchical, collaborative, directed C2, supplemental.

created by a central entity responsible for end-to-end GIG operation (e.g., JTF-GNO appointed by the U.S. Strategic Command). These policies become more detailed as they go to lower levels. These detailed policies and local observations decide the actions to be taken. This approach seems promising in creating a scalable

solution to the complex challenge of managing a network of very diverse networks to achieve the end-to-end objectives of the GIG. APL should continue to enhance this approach and take it to its natural conclusion.

While each network domain doing its own set of FCAPS (fault, configuration, accounting, performance, and security) functions for the network it administers can meet some of the network management needs, and the hierarchical PBNM discussed above will add some degree of central decision making and allow end-to-end coordination while keeping execution distributed, it will still not meet all the needs of a mission-oriented network of networks like the GIG. In particular, the short-term communications needs of a mission, if of significant magnitude, may not be anticipated by longer-term planning and long-term policies. Mission awareness may be at one or a few places at a higher level of the hierarchy. Meeting changing needs may involve actions at various levels and may even include the deployment of additional capacity (e.g., using communications relays like UAVs or ground robots). The need for actions of certain types may be based on end-to-end situation awareness at a higher level. However, specific actions to achieve the goal may be decided locally. This leads to hierarchical C2-based network management to supplement the hierarchical PBNM (Fig. 4b).

The mix of hierarchical C2 and hierarchical PBNM provides a very rich system that can scale to the GIG while allowing enough centralized controls where needed. APL has developed this concept and should continue creating details, making engineering choices, and architecting them in the overall network management architecture for the GIG. As with QoS and routing, the concepts of SCDs, SCD-SLCs, and R-SLCs will be useful in architecting this mixed approach. In particular, SCD-SLCs and R-SLCs provide succinct forms of network situation awareness and allow a higher-level network management system to identify actions needed (for mission management) and communicate them to action points.

An important challenge for the GIG network management system is managing infrastructure mobility. Whole networks, especially in deployed tactical environments, move and attach to the rest of the GIG at different places. How do we manage the dynamics of interconnection? How do management systems attach themselves after the network elements interconnect and maintain continuity of sessions, service-level agreements, etc? These issues are becoming important for APL to research and resolve.

Managing Mission-Oriented Networking

Although we discussed mission-oriented networking earlier, it needs a discussion of its own. Even for commercial needs, the Internet infrastructure lacks mission and end-to-end situation awareness. In fact, the core of

the Internet is deliberately kept ignorant of the applications and missions being supported. This philosophy has enabled Internet scalability and rapid service creation capabilities. However, many private enterprises have found this ignorance very limiting and have created their own systems to provide end-to-end situation and mission awareness. These tend to be proprietary or heavily manual and deal with the long-term business mission of an enterprise. The relatively small scale of a typical enterprise allows it to use networking experts to create manual procedures and provide mission-oriented controls and management.

Some of these approaches may be useful for the GIG if they can be automated and scaled to the GIG size. However, the GIG needs to be mission aware on several different scales, and the current enterprise solutions apply to only some of them. In particular, missions may be very long term (many years), medium term (e.g., months), or short term (hours and days). Mission knowledge may be available throughout the GIG or only to the highest levels of the GIG hierarchy. Missions may be very dynamic and may change as a result of the outcome of earlier actions. Different degrees and granularities of situation awareness are needed to meet the needs of these different mission types. Missions may also have widely varying needs on different dimensions of security. For example, some missions must have a very high degree of availability but minimal concern about confidentiality, while others cannot afford to have any "leaks."

Creating capabilities in the network and services infrastructure to meet the needs of all of these mission types is a challenge. The solution will impact QoS, routing, network management, and IA solutions. For example, a mission may need rapid capacity deployment in a specified geographical area. It may need rerouting to reconfigure the capacity distribution. It may have to reroute to change the security profile or reprioritize different applications and user communities. It may even need special treatment for some traffic types. For example, some critical mission traffic may need solutions involving multiple different paths and sending messages simultaneously on those paths to ensure a very high probability that at least one copy will reach the destination. These capabilities are beyond what the public Internet or private intranets provide today. The concepts of SCDs, SCD-SLCs, R-SLCs, QoS, hierarchical PBNM, hierarchical network C2, and Broad Sense QoS all will play roles in creating solutions.

APL has already begun to design solutions along these lines. There has been an external research push to study some aspects of this problem. In particular, there is significant interest in creating a knowledge plane overlay where situation awareness and mission knowledge are brought together to decide on mission-oriented control actions. APL should participate in this and related research activities, bring our insight to create

innovative solutions, and also leverage the work done by others in these initiatives.


CONCLUSIONS

The DoD, intelligence, homeland security, emergency response, and law enforcement communities are all aiming to use the power of the Internet and web to transform the way they do business. However, they all face technical challenges in realizing these goals. Some of these challenges arise from the more demanding application mix, while others stem from a more dynamic and possibly hostile communications environment. In this article, we have highlighted key challenges that APL can aspire to address to help our sponsors realize these ambitious goals.

REFERENCES

- ¹"The Army's Bandwidth Bottleneck," study sponsored by the Congressional Budget Office (Aug 2003); <http://ftp.cbo.gov/showdoc.cfm?index=4500&sequence=0>.
- ²Bayne, J., and Paul, R., "Scale-Free Enterprise & Control—Unified Command Structure," in *Proc. 10th Int. C2 Research and Technology Symp.*, Mclean, VA (13–16 Jun 2005); <http://www.dodccrp.org/events/2005/10th/CD/track05.htm>.
- ³Frankel, M., "Implementing the Global Information Grid," in *Proc. IEEE MILCOM*, available on CD (2003).
- ⁴Mazzei, J., and Bartko, A., "MUOS Integration into the DISN Infrastructure," in *Proc. IEEE MILCOM*, pp. 307–310 (Oct 2002).
- ⁵Melby, J., "JTRS and the Evolution Toward Software Defined Radio," in *Proc. IEEE MILCOM*, pp. 1286–1290 (Oct 2002).
- ⁶Sharret, I., "WIN-T—The Army's New Tactical Intranet," in *Proc. IEEE MILCOM*, pp. 1383–1387 (Nov 1999).
- ⁷Doshi, B., Benmohamed, L., and DeSimone, A., "A Hybrid End-to-End QoS Architecture for Heterogeneous Networks (Like the Global Information Grid)," in *Proc. IEEE MILCOM*, available on CD (2005).
- ⁸Doshi, B., Benmohamed, L., DeSimone, A., and Schmidt, K., "End-to-End QoS over the GIG," in *Proc. IEEE MILCOM*, available on CD (2004).
- ⁹Burbank, J. L., and Kasch, W. T., "IEEE 802.16 Broadband Wireless Technology and Its Application to the Military Problem Space," in *Proc. IEEE MILCOM*, available on CD (2005).
- ¹⁰Burbank, J. L., and Kasch, W. T., "Cross-Layer Design for Military Networks," in *Proc. IEEE MILCOM*, available on CD (2005).
- ¹¹Benmohamed, L., Chimento, P., Doshi, B., and Wang, I-J., "Design Considerations for Sensor Networks with Gateways," in *Proc. Multisensor Information Fusion Conf., SPIE Defense and Security Symp.*, available on CD (Mar 2005).
- ¹²Doshi, B., Benmohamed, L., Chimento, P., and Wang, I-J., "Sensor Fusion for Coastal Waters Surveillance," in *Proc. Multisensor Information Fusion Conf., SPIE Defense and Security Symp.*, available on CD (Mar 2005).
- ¹³Benmohamed, L., Doshi, B., DeSimone, A., and Cole, R., "Inter Domain Routing with Multi-Dimensional QoS Requirements," in *Proc. IEEE MILCOM*, available on CD (2005).
- ¹⁴Benmohamed, L., and Doshi, B., "QoS Routing in Multi-Level Multi-Domain Packet Networks," in *Proc. IEEE MILCOM* (2004) and *Proc. PACRIM05*, available on CD (2005).
- ¹⁵Haberman, B., "Connecting Enclaves Across the Global Information Grid Utilizing Layer-3 Virtual Private Networking Protocols," in *Proc. MILCOM*, available on CD (2005).
- ¹⁶Doshi, B., DeSimone, A., Small, S., Terzis, A., and Munrose, F., "Scalable VPNs for the Global Information Grid," in *Proc. IEEE MILCOM*, available on CD (2005).
- ¹⁷Doshi, B., "A Prefix Space Partitioning Approach to Scalable Peer Gateway Discovery in Secure Virtual Private Networks," in *Proc. IEEE MILCOM*, available on CD (2005).

THE AUTHOR



Bharat T. Doshi is a Gupta Endowed Chair Professor in Electrical and Computer Engineering at the University of Massachusetts, Amherst. From 2003 to 2005, he was Director of Transformational Communication at APL where he led many systems engineering working groups that contributed technical solutions to the development of the Global Information Grid (GIG) vision. Prior to his work at APL, Dr. Doshi spent 24 years at Bell Laboratories conducting personal research and research management, and worked in a wide range of networking technologies and applications. In July 2006, he will return to APL as Director of the Milton S. Eisenhower Research and Technology Development Center. Dr. Doshi has a B.Tech. from IIT Bombay, India, and M.S. and Ph.D. degrees from Cornell University. He received an Executive M.B.A. from the Kellogg School as part of a Leadership Continuity Program. He has applied for over 55 patents in the areas of converged networking, data networking, wireless networking, and communication protocols; of these, 38 patents have been granted. His awards include Fellow of Bell Labs (1996), Fellow of IEEE (1998), and the Distinguished Alumnus Award from IIT Bombay (2000). He is the author of over 120 published articles and associate editor of three journals. He has been the guest editor for four special issues of *IEEE Communications* and *Network* as well as two issues of *IEEE JSAC*. He has served on several government panels and advisory boards of universities and U.N. programs. His e-mail address is bharat.doshi@jhuapl.edu.