Networking: Technologies and Challenges for Network Centric Operations

Larry B. Stotts[a] , John G. Allen[b]
[a]Defense Research Project Agency, 3701 N. Fairfax Drive, Arlington VA, USA 22203;
[b]Booz Allen & Hamilton Inc., 3811 N. Fairfax, Drive, Arlington, VA 22203-1707;

ABSTRACT

This paper examines some of the challenges facing the community in providing radio communications to enable information systems for military operations. We believe that much of the on-going/completed work is necessary, but not sufficient, to provide the military Network Centric Operations, which integrates military's network centric enterprise with network centric warfare. Additional issues need to be addressed to better support battle commanders as well as decider-sensor-effector linkages. We discuss a possible way ahead.

1. INTRODUCTION

This paper examines some of the challenges facing the community in providing radio communications to enable information systems for military operations. In a companion paper [Reference 1], we discuss the essential differences between Network Centric Operations and network centric warfare, and the critical role of supporting battle commanders, as well as decider-sensor-effector linkages.

We are focused on supporting commanders at the operational level of warfare (commanders of carrier task forces, marine expeditionary forces, air wings, army corps/divisions) and the strategic level of warfare (joint force and components commanders). We also are dealing with the tactical level: commanders and leaders of brigades and battalions, squadrons and flights and individual ships.

Commanders are rarely inside the command post when crises occur. They may be in a mobile vehicle and have limited communications and computing capabilities. They are not bunched up but spread out over the deployed force, accessible by multiple communications networks. We will focus on the implementation of radio communications networks for these applications.

To limit the scope of the paper, we will not include Information Assurance but this function must be totally integrated into radio communications systems.

2. MILITARY APPLICATIONS OF RADIO COMMUNICATIONS

The military depends greatly on radio communications as well as on non-radio modes. To focus, we will consider a subset of four essential applications:

C2 = Command and Control – connecting commanders and leaders with each other and to sources of knowledge and understanding

CROP = Common and Relevant Operating Picture – disseminating a description of the battlespace to every commander, leader and warrior in a manner relevant to missions

D-S-E = Decider-Sensor-Effector links – connecting tactical decision makers and combat power, at the point of the spear, to enable forces to beat the enemy's combat execution cycle

ISR/TPAD links – connecting Intelligence, Surveillance and Reconnaissance sensors with the Tasking, Processing, Analysis and Dissemination segments.

Unattended/Unmanned Ground, Ocean, and Air Sensor Technologies
and Applications VI, edited by Edward M. Carapezza, Proc. of SPIE Vol. 5417
(SPIE, Bellingham, WA, 2004) · 0277-786X/04/$15 · doi: 10.1117/12.548185

Another critical application is local networks to connect distributed sensors; other papers at this conference will cover this.

The four applications we selected span a variety of characteristics as illustrated in Figure 1.

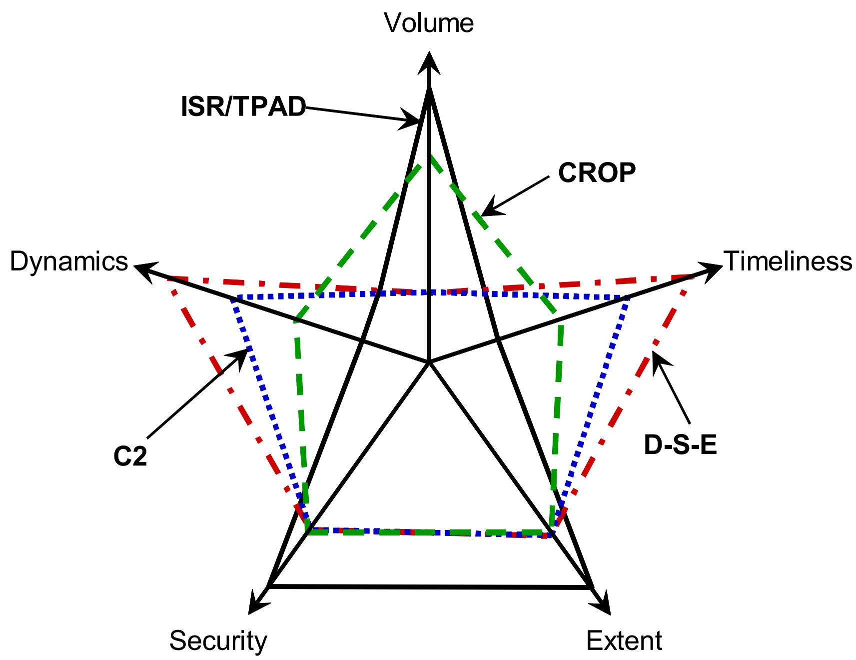

Figure 1: Application Variation

The dimensions included are:

- Dynamics - the degree of change in the geometry due to the mobility of the elements
- Volume – the quantity of communications the network must carry
- Timeliness – the latency allowed in communications
- Extent - the “distance” between the end systems involved in the communications
- Security – the protection needed from interception, exploitation and intrusion as well as deliberate and accidental interference.

For the mathematically inclined reader, the authors point out that the scale used in the figure is a highly complex, logarithm-based relationship, the details of which are too extensive for the limited number of pages available for this paper.

The largest volume of communications is associated with ISR/TPAD applications. The ISR sensors require large numbers of humans to perform the tasking, processing, analysis and dissemination (TPAD) functions. These TPAD people are highly trained and need to be kept in a safe haven, often in the CONUS. On the other hand, the sensors may be on deep penetrating airborne or space-borne platforms and will be widely separated from the TPAD centers. Thus, the communications occur over a large area with the need for a high level of security. On the other hand, the timeliness needed is not instantaneous, but "near real-time" and the dynamics of the communications links is relatively slow changing.

The other applications also can extend over large areas but do not involve the volume associated with ISR/TPAD. In a D-S-E link, the decider might be a special operations team, the sensor might be in on a Predator, and the effector might be naval gunfire – this can extend over a considerable area and the timeliness requirement is very high.

All of the applications have a requirement for a high level of security. So, in summary, the four applications show a large variation in their characteristics and consequently, there is a large variation in the performance required from the actual communications network. This indicates that the network must exhibit robustness; it must be able to adapt to a multitude of unpredictable situations and traffic flows.

3. EVOLVING INFRASTRUCTURE

3. 1 Global information grid

The Department of Defense is developing the Global Information Grid to interconnect all military forces and facilities world wide. The illustration in Figure 2 is taken from Reference 2 and the various acronyms can be found in the reference.

Here we see a tiered architecture. The lowest tier is the realm of tactical sensor-shooter networks implemented with small tactical radios and mobile ad hoc networking technology. The upper tiers provide the world wide / theater backbone implemented with high capacity space and air based platforms as well as terrestrial fiber-optics. In the middle, is the critical Tier 2 – the mobile backbone? Does this layer provide the interoperability between upper and lower tiers? This is crucial because lower echelon Joint Forces will have mixed radio structures for a couple of decades based on projected acquisition budgets. In our opinion, the answer is yes. Let us be more specific.

For Tier 2 to be truly a mobile wireless backbone network, it must fill the gaps between the upper tiers that employ a fixed terrestrial and space based infrastructure with the fluidly mobile lower tier comprised of ad hoc tactical networks and legacy radios, e.g., SINCGARS, HAVE QUICK, EPLRS, LINK 16. None of the latter map well into the TCP/CDMA format proposed for the upper tiers. DARPA is thinking about ways that power control in CDMA is not necessary to achieve improved network capacity.

Earlier, we described four classes of communications applications. Here we see that the entire GIG structure is needed to implement the communications services needed for these applications. They all require information to cross from one tier to another and in particular, to pass through Tier 2.

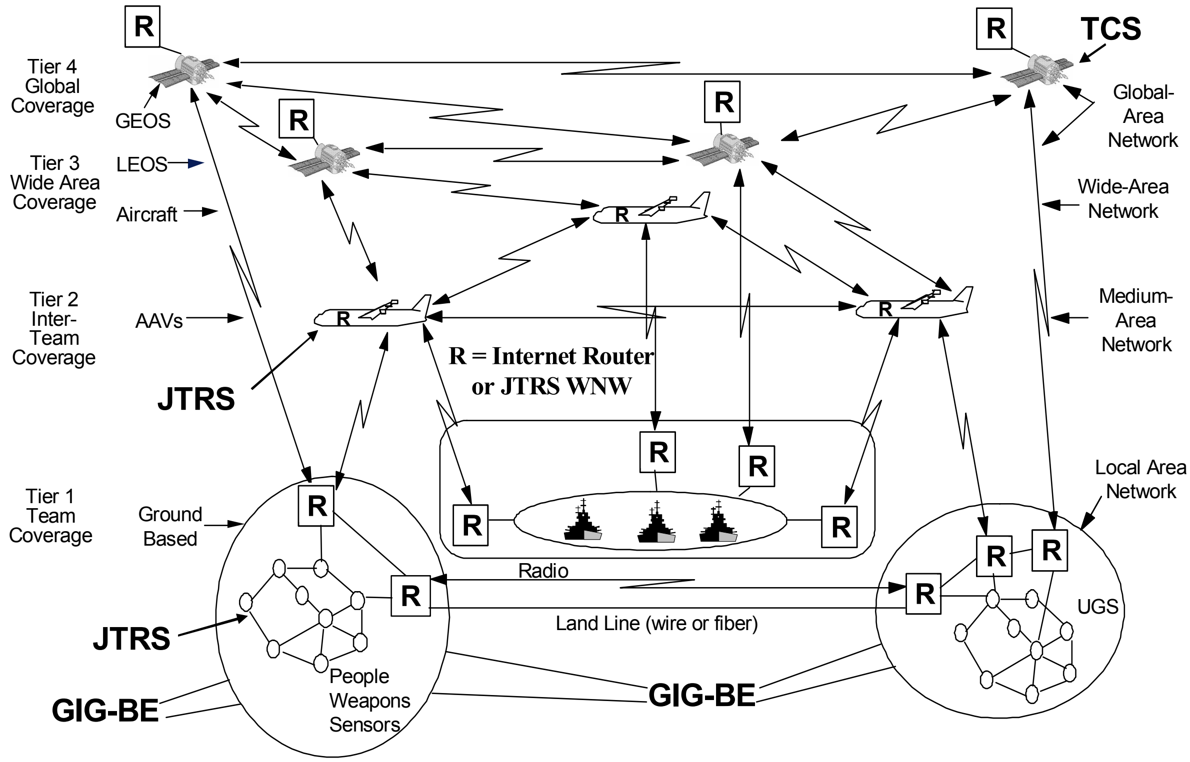

Figure 2: DoD GIG Architecture

3.2 Tier 2

In Figure 3, we have recreated a stylized view of the DoD GIG on the left highlighting the tiers. On the right, we show Tier 2 and its various connections to the other Tiers.

In terms of challenges, Tier 2 is where the metal really meets the mat! It consists of:

- Air-Space Links
- Air-Air Links
- Air-Ground Links
- Space-Ground Links
- Ground-Ground links

Tier 2 interconnects the communications traffic that crosses over these kind of links and between the other tiers. Tier 2 must support traffic with widely varying quality of service needs and transport/networking schemes.

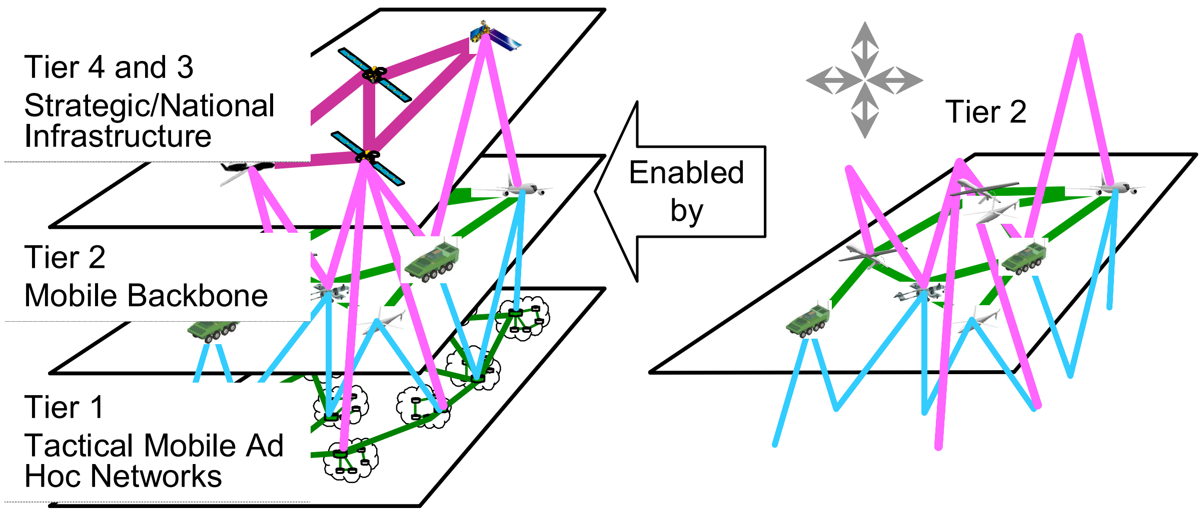

Figure 3: Tier 2

4. TECHNICAL CHALLENGES

Using the ISO open systems interconnection model of communications services, let's walk down the stack.

4.1 End system interfaces

The first area is interface with the commander's end systems, via the presentation, session and applications layers. Here is where "Quality of Service" really begins. To the commander, Quality of Service (QoS) translates into metrics like:

- Does critical information arrive when needed?
- When I push the fire button, does the effector act?

A challenge is in the area of compression. We're not talking about compressing data or images, but really extracting critical information – finding the golden nuggets in the tons of dross – and transmitting them efficiently to the Commanders. For example, we may send colored icons of potential targets, with the colors representing confidence levels (T72 tanks with a 70% confidence), rather than ISR data on the target. With the DoD losing bandwidth to the commercial sector, we need to minimize bandwidth use whenever possible.

Another illustration of this type of compression is provided by the manner in which humans interact at a conference table. There is a limited amount of "bandwidth available." Only one person can talk at one time or use the white board or use the projector. Everyone has a "model" of the others, what they know already, what they are interested in, how they react, and so forth. They use this model to control what they show and tell, and to decide when they need to show and tell.

4.2 Transport/Networking

One of the mantras today is the notion of “Viral Communications” in which every radio is allowed to and encouraged to join the network. The notion is that with large networks, link distances are shorter and this reduces the average transmitter power which in turn allows spectrum to be reused and recovered over shorter distances. *Unfortunately,* being a router increases energy consumption because the receiver must be active all the time. In addition, the capacity of the network to pass traffic across the network is reduced by an order of $\sim 1/\sqrt{n}$ [Reference 3].

Another mantra is that self forming ad hoc networks can seamlessly connect everyone on the battlefield. One draw back of this is that, inherently isolated clusters can be formed. The intra cluster links generally will have high capacity (soldier to soldier) while the inter cluster links will have low capacity (commander to commander). This is not the situation desired. Opportunistic topologies can’t ensure the service needed.

The challenge is to avoid the $1/\sqrt{n}$ problem and proactively manage network topologies [see Reference 4 for a discussion].

4.3 Link/Physical layer

“We need more bandwidth” is the cry of the communications community. An evolving mantra is that unused or seldom used spectrum can be harvested and used on an opportunistic basis. This is generally the way in which access to some unlicensed spectrum is controlled today, by use of etiquette or, for the NII bands, Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS). In the US, the FCC is considering the notion of “interference temperature:” and also considering making more spectrum available on an unlicensed basis using TPC/DFS [Reference 5]. DARPA is investigating this general area in the NeXt Generation (XG) program.

Gaining bandwidth itself is not the complete answer – the challenge is to find usable bandwidth. For Tier 2 especially, to support the link, transport/networking and application interfaces, we need good radio channels! We need channels that dependable and can support high capacity traffic.

The goodness of a channel depends on four qualities:

- *Availability* - can the channel be provided when needed and demanded or is it available on an unpredictable basis
- *Reliability* - will the channel remain available while it is being used or will it unexpectedly go down requiring the network to alter routing
- *Security* – can the cannel be trusted or is it susceptible to intrusion, exploitation or jamming
- *Service Offered* – does the channel provide an adequate data rate for actual transmission of data or does it require a tremendous overhead to maintain itself?

The last quality is of course partially related to bandwidth, but the others are not.

In sharing spectrum, it is recognized that special provisions are needed to avoid the “Tragedy of the Commons.” This is the phenomena, coined by Garrett Hardin, in which, when demand exceeds resources, individuals will attempt to increase their usage at the expense of the common good. A challenge will be to develop protocols and etiquettes to prevent low priority data from swamping the network. In military communications, there is the need for a priority/precedence scheme that enables commanders to seize communications when absolutely needed. There also is the challenge of ensuring this kind of Quality of Service.

Another mantra circling about is that the military can exploit commercial wireless technology. This is partially true in that the commercial world is full of creative individuals who create sophisticated protocols. The commercial world also is a source of low cost, very sophisticated devices. However, commercial products generally do not provide the Security, Protection and Availability (SPA) needs for military applications. In addition, the commercial world does not have a Tier 2 equivalent at the link and physical layers. The commercial world relies on the fixed, stable, extensive Internet as the backbone and has only to contend with the “last mile” or so in a wireless mode. True, there is some long range wireless technology available for backhaul applications and development of long range metropolitan wireless network standards is underway (e.g., IEEE 802.16). Generally, however, the waveforms adopted for commercial applications can not support the SPA requirements for Tier 2. They are inherently, periodic, predictable and use preambles, the three characteristics that must be avoided for transmission secure waveforms.

5. DARPA'S POSSIBLE WAY AHEAD

At DARPA, to organize ourselves, we have developed a canonical architecture of the C4ISR process with a distinction between Command and Control (C2) and Communications, Computers, Intelligence, Surveillance and Reconnaissance (C2ISR). Again, refer to Reference 1 for the details. One version of our architecture is depicted in Figure 4.

Here we see the commanders and tactical deciders interacting with one another (C2 links) and with sources of understanding and knowledge (CROP). Decider-Sensor-Effector links are also shown as well as the ISR/TPAD links.

This view of the architecture highlights several considerations. As we move up, data is converted into information and then knowledge and finally "understanding" that enables commanders to internalize the battlesphere situation and select their course of action. During this process, the volume of communications data is greatly reduced. The commander is now attached to an understanding source rather that being attached to numerous sources of low level data.

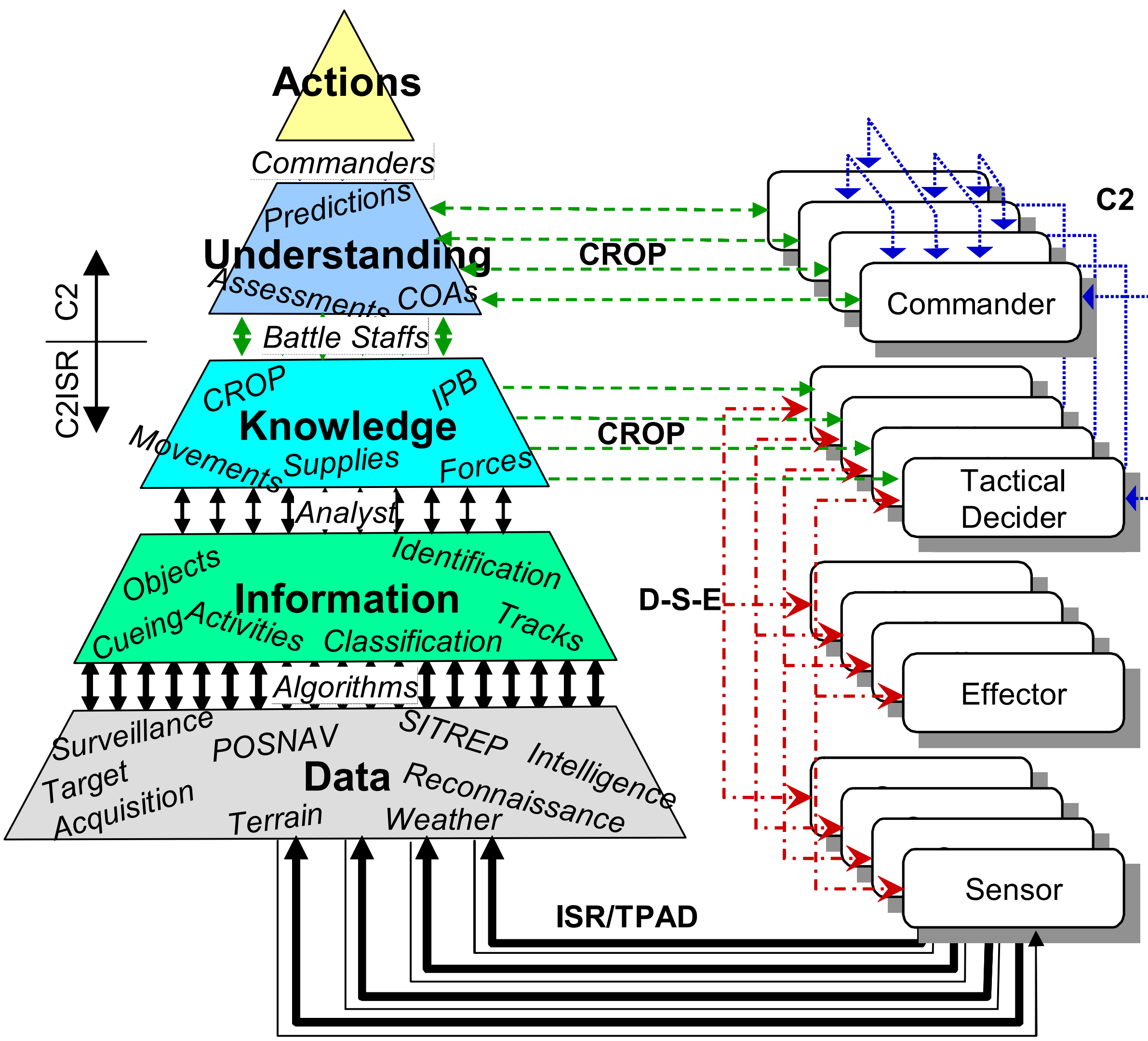

Figure 4: Canonical C4ISR Architecture

6. CONCLUSION

This paper examined some of the challenges facing the community in providing radio communications to enable information systems for military operations. We believe that much of the on-going/completed work is necessary, but not sufficient, to provide the military Network Centric Operations, which integrates military's network centric enterprise with network centric warfare. Additional issues need to be addressed to better support battle commanders as well as decider-sensor-effector linkages. We discussed a possible way ahead.

References

1. Achieving Joint Battle Command in Network Centric Operations, L.B. Stotts, et al., this publication.

2. Implementing the Global Information Grid, (GIG), A Foundation for 2010 Net Centric Warfare (NCW), Dr. Michael S. Frankel, DASD(C3ISR, Space & IT Programs), 27 June 2003, briefing available from http://www.dodccrp.org/8thICCRTS/Pres/plenary/1_0915frankel.pdf

3. The Capacity of Wireless Networks, P. Gupta and P.R. Kumar, IEEE Trans. On Information Theory, **46**, 2, March 2000

4. Performance and Scalability of Mobile Wireless Base-Station-Oriented Networks, S.D. Milner, S Thakkar, K. Chandrashekar and W. L. Chen, University of Maryland, undated.

5. Notice of Inquiry and Notice of Proposed Rulemaking, Establishment of an Interference Temperature Metric to Quantify and Manage Interference and to Expand Available Unlicensed Operation in Certain Fixed, Mobile and Satellite Frequency Bands, Federal Communications Commission, ET Docket No. 03-237, Adopted: November 13, 2003.