Networking for Network Centric Operations: Technologies and Challenges

Dave Honey[a], Larry B. Stotts[b], Paul Kolodzy[c]
[a,b]Defense Research Project Agency, 3701 N. Fairfax Drive, Arlington VA, USA 22203;
[c]Kolodzy Consulting, PO Box 1443, Centreville, VA 20120

ABSTRACT

This paper examines some of the technologies and challenges facing the community in providing robust communications for the network-enabled command, control and information dissemination needed for successful Major Combat Operations (MCO), Security and Sustain Operations (SASO) and other military operations in the future.

Keywords: military mobile networking, multi-level security, spectrum efficiency

1. INTRODUCTION

The after-action analysis of the command and control systems from many of the conflicts since Vietnam indicated a consistent inability to communicate between the services during joint operations and exercises. After Grenada, a GAO report[1] indicated that air support operations between the Army ground forces and Marines were hampered due to the incompatibility of their radios. These shortfalls continued though to the 1990 Persian Gulf War as described in a 1992 report to Congress[2,3] that described the problems in establishing an interoperable network across disparate communications systems. Interoperability enables information to be exchanges among the services directly and satisfactorily. These same issues are also prevalent in the non-DoD communications systems used for public safety organizations as seen during the response to the terrorist attacks of September, 2001.

Early in the 21st Century, the focus of many of the DoD efforts was on how to enable Network-Centric Warfare (NCW). In particular, NCW was to allow warfighters to take advantage of all the available information within the Battlespace in a rapid and flexible manner. One example is the enabling of an effective the sensor-to-shooter process. The key enabler to this process was development of the Global Information Grid (GIG)[4]. The GIG is the network fabric for which to build a "Systems of Systems". Mobile networking is one piece of the GIG and is built upon the use of the proposed interoperable Joint Tactical Radio System (JTRS).

This paper examines some of the technologies and challenges facing the community in providing robust communications for the network-enabled command, control and information dissemination needed for successful Major Combat Operations (MCO), Security and Sustain Operations (SASO) and other military operations in the future. This examination focuses on the Department of Defense's extension of the Global Information Grid (GIG) to the tactical edge using the Transformational Communications Architecture.

Defense Transformation and Network-Centric Systems, edited by Raja Suresh,
Proceedings of SPIE Vol. 5820 (SPIE, Bellingham, WA, 2005)
0277-786X/05/$15 · doi: 10.1117/12.608424

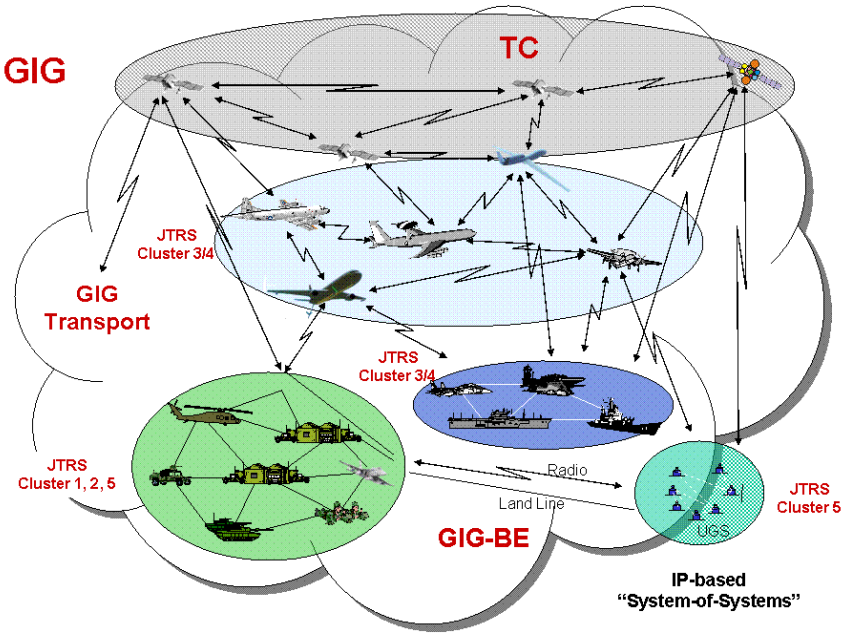


Figure 1: Joint Network Vision

Figure 1 illustrates the Department's Transformational Communications vision, which includes the GIG extension[5]. The Department's objective is to connect the Network Centric Enterprise to the Network-Centric Tactical forces seamlessly when complete. The Services' and Combatant Commands' objectives are better shared awareness, understanding, collaboration and synchronization among commanders at joint, coalition and lower echelon levels. The intent of this paper is to highlight the envisioned architecture and discuss issues that we think need to be addressed in order to achieve the above objectives.

2. EVOLVING INFRASTRUCTURE

2.1 Global Information Grid

Today, the Combatant Commanders have two distinct parts to their command, Network Centric Enterprise and Network Centric Warfare. Their basic attributes are shown in Figure 2. The Department of Defense is extending the GIG to interconnect all military forces and facilities world-wide. The basic architecture[6] is shown in Figure 3, which is taken from Reference 2 and the various acronyms can be found in that reference. It is apparent from Figure 3 that Transformation Communication Architecture (TCA)[7] is a tiered architecture. The lowest tier is the realm of tactical sensor-shooter networks implemented with small tactical legacy 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 specific terms, the GIG extension basically is a homogeneous network, based on Internet Protocol Version 6 (IP v6) and wideband Code Division Multiple Access (CDMA), to seamless interconnect the various entities. This approach was chosen to leverage for the military the success of the Internet providers to provide timely data search and dissemination to their commercial customers.

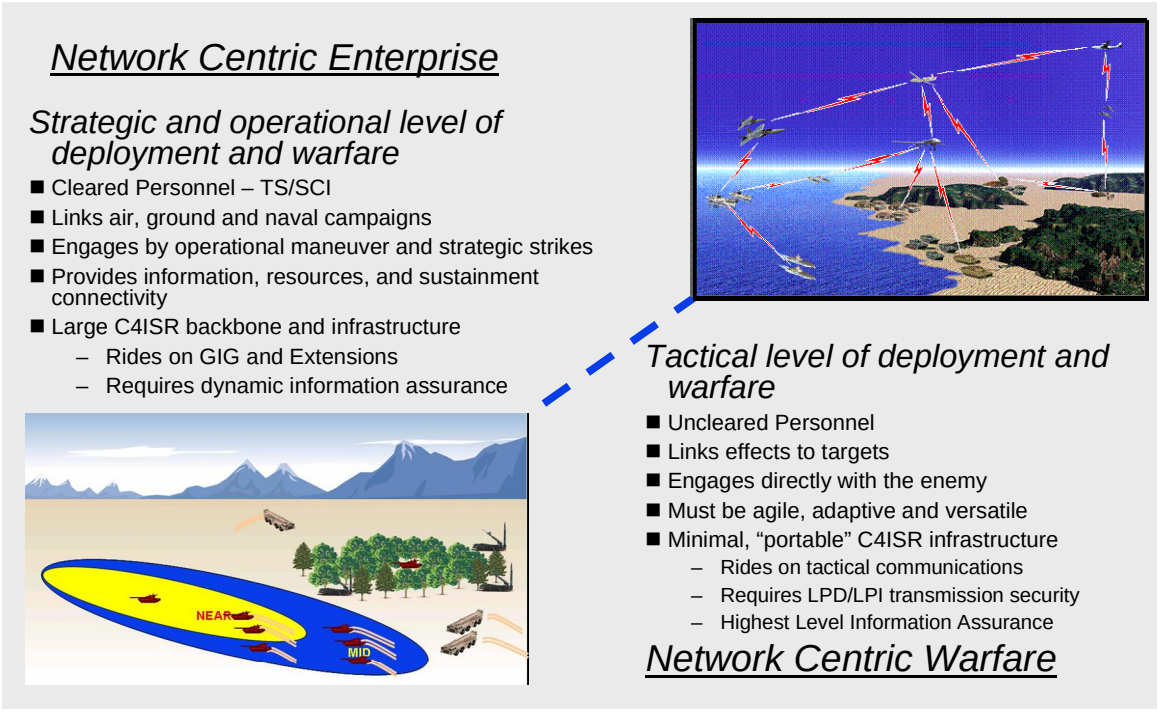


Figure 2: Military Operations Structure – Enterprise and Tactical Warfare

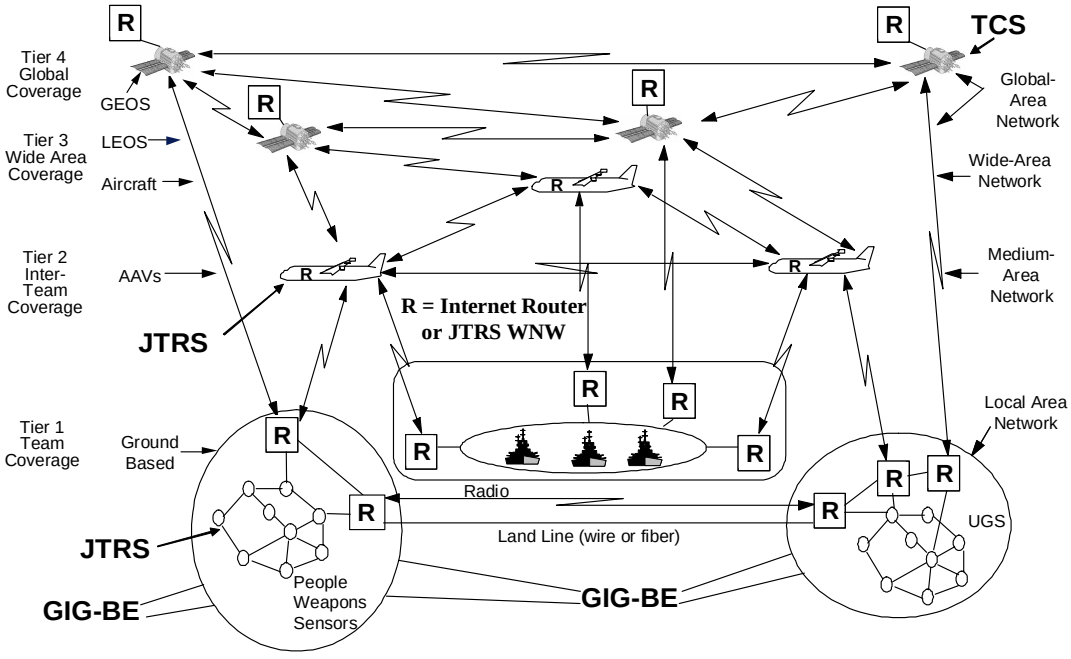


Figure 3: Transformational Communications Architecture Overview

The upper layers use Free-Space Optical and Extra High Frequency communications interconnects the various nodes in the Tiers 3 and 4. As one transitions from Tier 3 to Tiers 2, the Joint Tactical Radio System (JTRS) takes over as the interconnect mechanism between Tier 2 and 3, and among the various nodes of Tier 2 and Tier 1. This is mainly because of weather, interoperability and other considerations. In short, IP v6 / CDMA is network / access protocol for all tiers and the basis for the network's homogeneous nature, and JTRS Cluster 5, the Wideband Network Waveform (WNW) system, must be interchangeable with IP v6 routers to facilitate seamless interoperability between the other JTRS Clusters and current legacy systems.

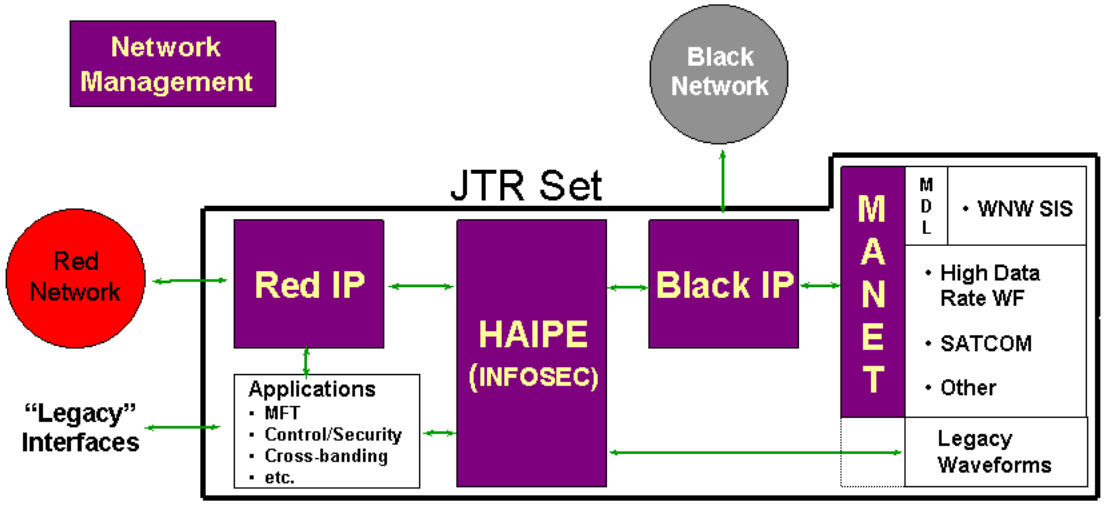


Figure 4: The JTRS Architecture

This last point is better illustrated in figure 4, the JTRS architecture. WNW disseminates seamlessly the incoming traffic from the GIG extension network to other radio systems though a Mobile Ad hoc NETwork (MANET) and other entities. WNW is there because most MANETs, legacy and teleport systems are not directly, seamlessly TCP/IP compatible. Underlining the TCA is the assumption that there is sufficient spectrum available, like the commercial world has, that allow the large, timely data search and dissemination, as well as other unique military services.

3. TECHNICAL CHALLENGES

In this section, we will discuss the technologies and challenges in this approach and our view on some constructive changes that would address our concerns. There are many instances of the migration path to network centric warfare places emphasis on wired architectures transitioning to wireless. Mandating IPv6 protocols for *all* networked systems, high degree of physical layer agility, and cryptographic standards that are independent of the physical limitations and the system dynamics can create a process in which there will be highly suboptimal systems being developed.

Mobile networks, or wireless communications networks, are very different from stationary, wired networks. The first difference is in availability of communications resources: bandwidth, spectrum, and power. Each of these resources places a trade between the means in which to achieve interoperability and the available of those resources. The use of "wired-centric" protocols leads to highly bandwidth and power inefficient systems. The second difference is the stability of the network and the availability of resources to maintain the network fabric.

3.1 Spectrum Availability for Military Networks

The GIG is fixed infrastructure network that uses fiber-optics, with wavelength agile sources, to provide the high capacity network communications and data dissemination among users. Based on today's commercial technology, we have the situation shown in Figure 5. Based upon the technology for dense wave division multiplexed (DWDM), a single optical bundle can carry 12,800 GHz of optical signal. Therefore, a single optical bundle can carry 4000 times the traffic

compared to the 3 GHz of RF spectrum that is readily usable for mobile communications. Therefore there is significantly less spectrum for mobile networking than for infrastructure-based, fixed wired networking.

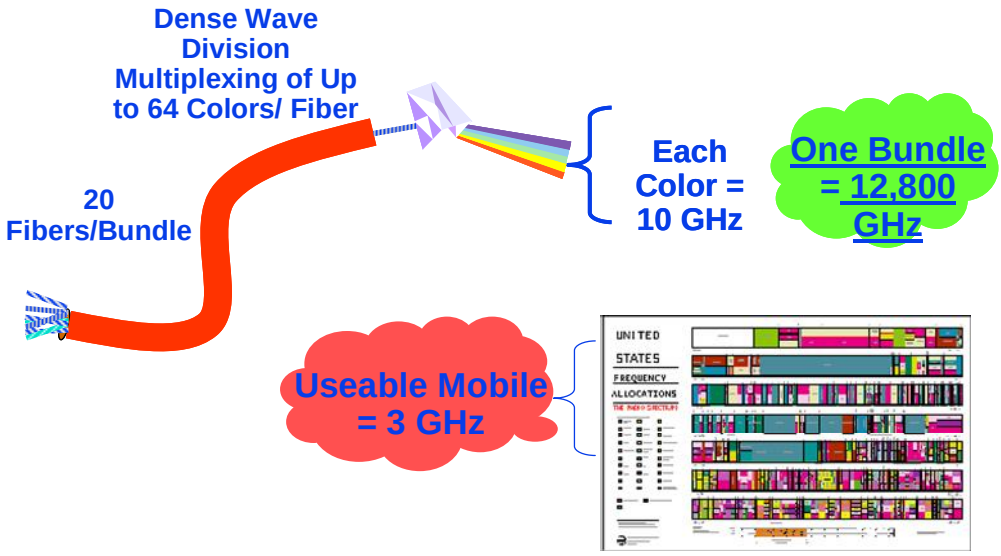


Figure 5: Bandwidth Capacities of Fiber and Wireless Mobile Communications

Additionally, military networks have additional constraints due to the expeditionary operations that must be addressed. Current spectrum allocation provides less than 20% of the spectrum less than 3 GHz for military networks within the US. When overseas, the US military must negotiate access to spectrum with the appropriate government(s) agency(ies). The outcome is significantly less than the 20% afforded in the US. The RF bands also may have some mismatch to those necessary for the equipment under deployment. This translates into a reduction is systems deployed or limited capability to the systems that are deployed.

The lack of spectrum resources can be significantly limiting to mobile military networks. As we will describe in the following section, the overabundance of infrastructure-based, wired spectrum has helped in the creation highly spectrally inefficient protocols that are being transferred to the mobile networking with little regard to the limits of spectrum.

3.2 Bandwidth Efficiency

In the last few years, there has been a movement emerging for the military to exploit commercial wireless technology. Ignoring the fact that commercial products generally do not provide the Security, Protection and Availability (SPA) needs for military applications, there are some organization like the Naval Postgraduate School investigating various long range commercial wireless technologies available for backhaul applications and long range metropolitan wireless network standards, e.g., IEEE 802.11. There assumption is that SPA will eventually be developed by commercial industry that will meet the Department's SPA requirements.

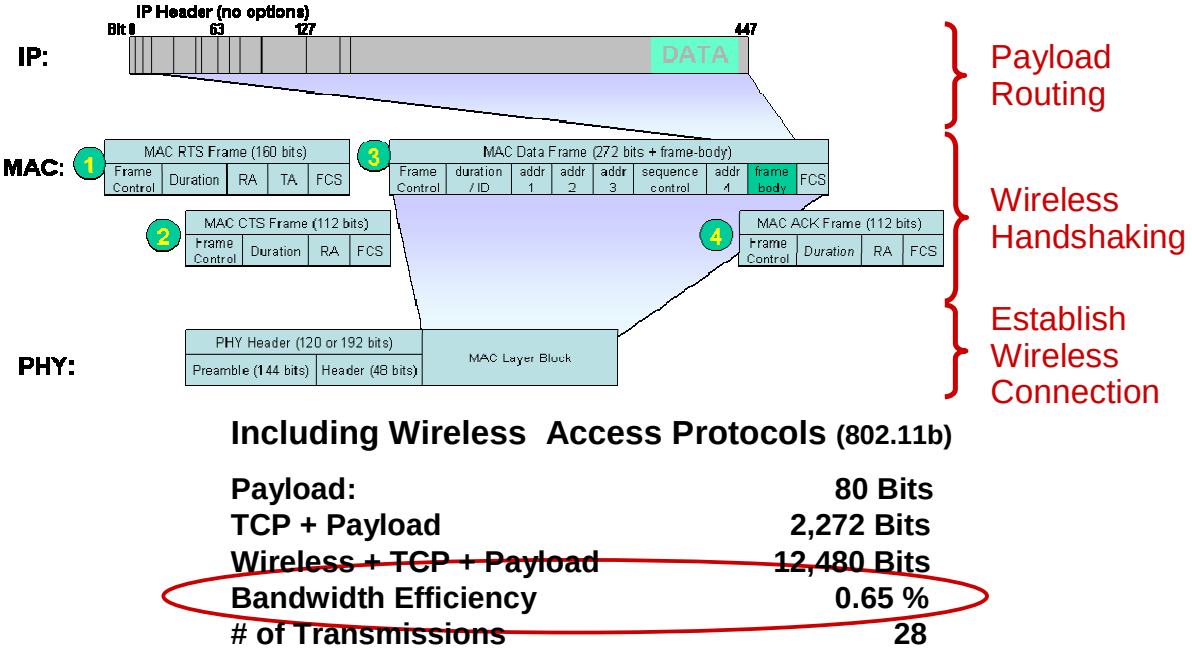
In the previous section, we saw the amount of available spectrum for network communications in the TCA wireless infrastructure is significantly less than that available in the fixed GIG infrastructure. This means that frequency reuse must be employed to essentially expand the amount of available spectrum for networking. In other words, the implication is that we need to work on ways of better sharing that limited, very valuable, resource, e.g., DARPA's Next Generation (XG) Program.

Commercial industry has successfully achieved better spectrum sharing by their approach to cellular telephone, e.g., cell towers coupled with CDMA (IS-95). This is just the beginning of our move to picture / movie phones and other high data rate wireless applications, which will require better protocols to meet their high capacity networking demands, e.g., Third Generation Wireless, the hybrid of Time Division Multiple Access and CDMA.

The Department has the vision that because of the success of commercial wireless, we can use commercial protocols to provide communications down to Tier I entities like unattended ground sensors and dismounted forces (See Figure 1).

The implicit assumption is communications within the network is done as efficiently as possible, given the discussion in the previous subsection. Is this a good assumption? Let look at the bandwidth efficiency of a TCP/IP link using a popular wireless protocol, 802.11. Assumed here is that there are many subscribers fighting for use of the limited spectrum and will not be on the interacting with the network continuously because of operational and/or spectrum reuse / sharing reasons.

Figure 6 shows the efficiency for a 80-bit payload that may come from an unattended ground sensor (UGS). Due to the low transmission duty cycle from an UGS, the TCP networking connection handshakes need to be completely executed as well as the wireless carrier-sensing, multiple-access (CSMA) media access and control (MAC) handshakes. Therefore, a total of 28 transmissions need to be sent for a single data packet. The number of additional header information for the TCP/IP protocol and the additional physical layer and MAC headers utilizing 12,400 bits for 80 bit payload.



Including Wireless Access Protocols (802.11b)

Payload:	**80 Bits**
TCP + Payload	**2,272 Bits**
Wireless + TCP + Payload	**12,480 Bits**
Bandwidth Efficiency	**0.65 %**
# of Transmissions	**28**

Figure 6: Bandwidth Transmission Efficiency for 802.11b for 80-bit Sensor Payload

The NCW model of data networks inclusive of sensor networks assumes that a large number of transmissions utilizing these protocols. Given the limited spectrum availability of the previous section, the current protocols will not be affordable spectrally.

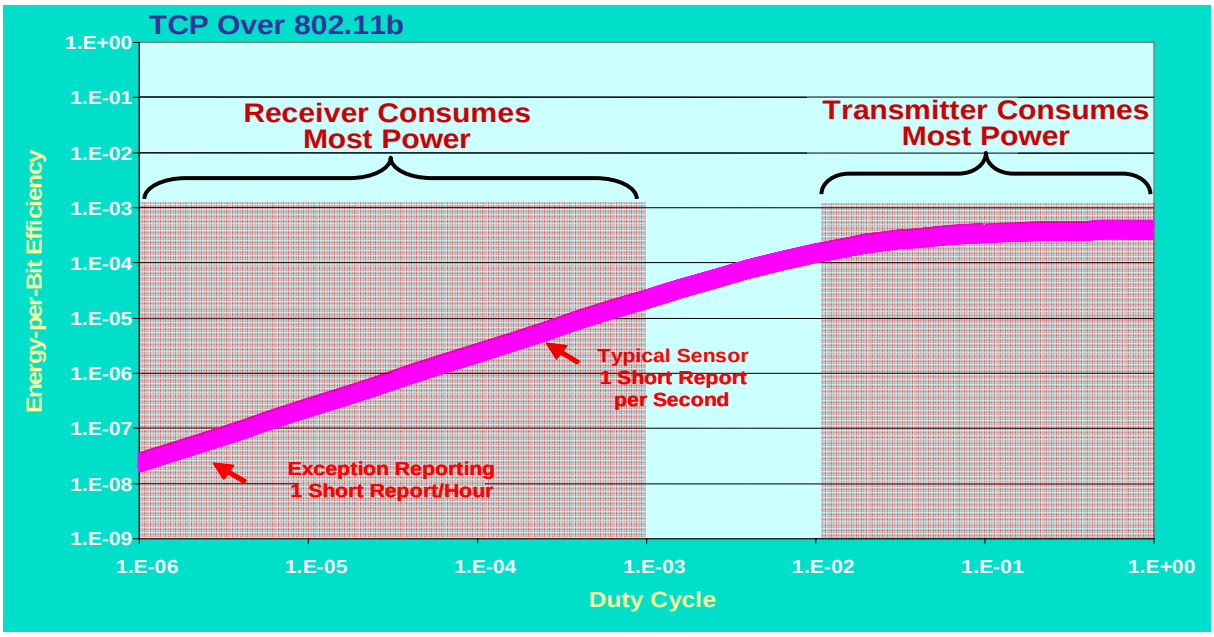


Figure 7: Power Efficiency of Wired Protocols for Low Duty Cycle Communications. Unattended Ground Sensors are dominated by Power to Continuously Operate the Receiver

3.3 Power Efficiency

The current commercial and military communications networks, as shown in the previous section, are very inefficient with bandwidth. We are also seeing a transition from transmitter-dominated power consumption to receiver-dominated power consumption. This is due to the rise in both the complexity of the receivers to address waveform complexity, and to the low duty cycle transmission patterns for sensor networks. Although there are no transmissions, receiver is constantly searching for signals. This effect gets more pronounced as the transmission duty cycle is reduced.

Keeping with the 802.11b model, Figure 7 shows the impact as energy per bit efficiency value[8] with 0.65% as being the upper limit as shown in Figure 6. Duty cycle for UGS can be easily as low as 10^{-5} which is equivalent to 1 information packet every 100 seconds.
The future sensor networks are highly reliant on power efficiency for longevity. The use of wired or wall-plug powered wireless system communications protocols will severely limit UGS longevity and utility in the battlefield.

3.4 Heterogeneous Networking

The current wired internet is based upon a common internet protocol and a robust routing table capability. Routing tables are fairly static and change only over long time scales[i]. Therefore, the technology that has been developed has exploited the static, homogeneous characteristics of the wired internet. Mobile networks exhibit significant number of differences to the wired internet. Mobile networks are actually a Network of Networks in both physical instantiations and in network structure. Mobile networks operated and interface between Unattended Ground Sensors, pedestrians, ground vehicles, low altitude aircraft, ships, high altitude aircraft, and satellite platforms. Each platform has different characteristics in mobility, available power, line-of-sight, latency tolerance, etc. Each of the platforms will exhibit differing networking requirements and place challenges on the interfaces between them.

Network of Networks architectural challenges are in three operational domains: within an individual network, within network-to-network connectivity, and between coalition networks.

[i] Mobile IP is a solution for introducing mobility for IP and routing tables. It uses an intermediate device/server to allow the routing tables to remain static and that the end-point addressing is morphed to a temporary IP address to reflect it current attachment point in the network. In essence, it has two IP addresses: one static, one dynamic.

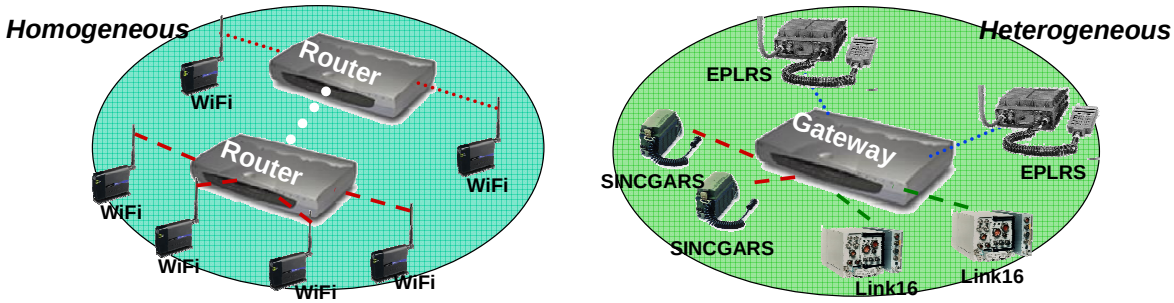


Figure 8: Homogeneous Networks Architectures Employ Routers vs Heterogenous Military Mobile Networks Employ Gateways between Disparate Networks

Scalability for data routing is the primary challenge for within a mobile network. The mobility will create topology changes and thus require a serious demand on network resources to maintain accurate routing tables. Military systems, especially UGS and dismounted soldiers, represent the greatest challenge due to serious power limitations as well as the need to scale to 1000's of nodes.

The Network-to-Network connectivity challenges have the additional challenge of disparate physical layers between the networks that will require real-time, continual adaptation and conversion between RF/Optical waveforms and protocols. This problem distinguishes between routers for transport between similar networks and gateways for transport across different networks as depicted in Figure 8. An example of a router would be WiFi to WiFi networking, cellular telephony to cellular telephone networking. The physical and MAC layers would be similar with potentially differing protocols such as TCP, UDP, SCTP, etc. A gateway connects disparate nodes with differing physical attributes, waveforms, and protocols. Gateways have the capacity to bridge between differing networks such as infrastructure based, ad hoc, mobile ad hoc network (MANET), etc.

A potentially more serious Network-to-Network challenge is the routing and quality of service (QoS) constraints[ii] when attempting to route across networks with different capacities. The problem of transmitting a video stream across a Mbit/sec link followed by a Kbit/sec link needs to be addressed. However, should it be addressed by the application layer (i.e. send less bits across the network via judicious selection), network layer (i.e. reduce the number of bits at the high-low bandwidth interface), or just to let the QoS be exceedingly poor.

Finally, more relevant situations are the challenges to operate coalition networks. In this case, the waveforms and protocols are not common and thus negotiations are needed within the physical, MAC, and network domains. Routing, especially for secure communications, becomes problematic. Coalition partners may not wish to provide detailed routing information of there network to a potentially untrusted partner and thus new schemes are needed to provide a useable networking interface.

Again, heterogeneous mobile networking systems limit the utility of networking architectures developed for homogeneous systems. Current router technology does not provide the interoperability between heterogeneous networks. New techniques that can discover, translate, and negotiate within gateway-level architecture are becoming necessary.

3.5 Secure InterNetworking

The advent of mobile networks and unattended sensor and communications nodes has helped to reshape the requirements for secure networks. Three, previously separate, security domains need to be integrated in order to provide both the security and the flexibility in the operations of mobile networks: Secure Communications Transmission (COMSEC/TRANSEC), Information Assurance (IA), and Multi-Level Security (MLS).

The challenges in this integration are the basic assumptions that are invoked for each of the security domains. COMSEC focuses entirely on each individual wireless link to ensure that the communications are either not detectable or cannot be demodulated. It does not, in general, address the multi-user access systems and thus it trades communications resources (bandwidth and computational power) for security.

[ii] e.g. latency data rate, jitter

Information assurance focuses entirely on the network to ensure that access by unauthorized users is limited and, if granted, can be detected. If detected, then the impact of the unauthorized user to the network will be limited. The origins of IA technology are generally to the wired, non-mobile, internet. Therefore, many of the techniques developed assume a large bandwidth and computational capability. The physical attributes of the communications channel are generally neither addressed nor exploited.

Multi-Level security is a very specialized domain in processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. MLS addresses both the intra-node security and inter-node security. Intra-node MLS has focused on verifiable software-based solution to isolate processing at different security levels and the appropriate interfaces to transfer information from one level to another. The verification process is extremely labor and time intensive which creates gaps between the capability of the verified software and new processing and algorithmic capabilities. The inter-node MLS focuses on the manual (man-in-the-loop) determination of security levels or operation at the highest level of security.

The wireless portion of the GIG will includes mobile networks that will interoperate with a large number of unattended sensors. The amount of wireless devices will soon outnumber the number of combatants and obtain most of their utility from the ability to network and share and combine data. As mentioned earlier, the amount of spectrum/bandwidth resources are limited within the battlespace and thus the techniques that have generally been develop for the COMSEC and IA communities will not be applicable. Secure mobile networking will require these communities to combine and develop the security technology that is cognizant of the networking and higher levels of communications necessary using the finite spectral resources.

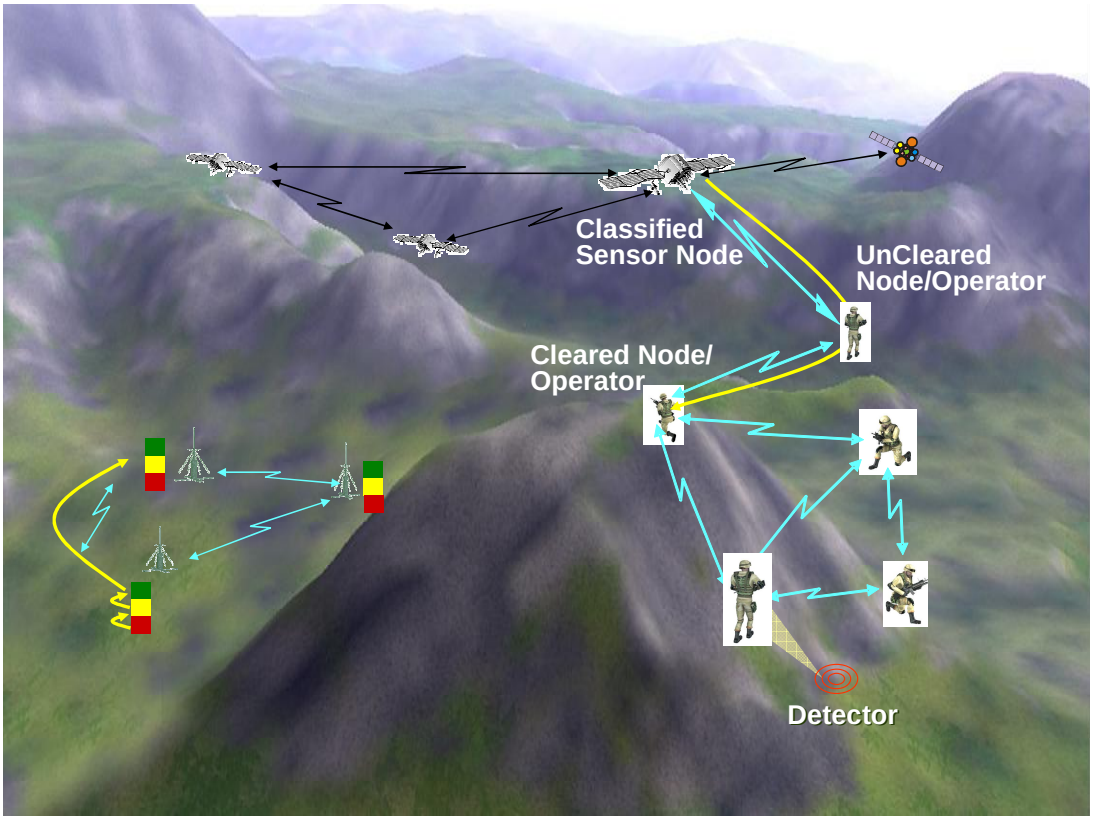


Figure 9: Secure Internetworking Challenges for Network Centric Warfare

Additionally, new low-power, agile sensors has now spurred the development of a new class of unattended systems that have very sophisticated capabilities. Some of the new systems can perform the mission of many stand-off systems and require classified information to perform their function. Therefore within a single, unattended node there are multiple

levels of classified processing. More importantly, these systems are enhanced through networking and eventually connect to the command and control (C2) system. Figure 9 illustrates the challenges for MLS in a mobile networking environment. The sensor field on the lower left indicates the need operating across multiple classification levels (red, yellow, green) within a node as well as operating between nodes. The right side of the figure depicts the challenge of having classified sensor nodes passing specific targeting information through an uncleared node to get to the destination node that is cleared for that level of information. Therefore, a mechanism for black-side MLS is needed within the JTRS architecture as is shown in Figure 10.

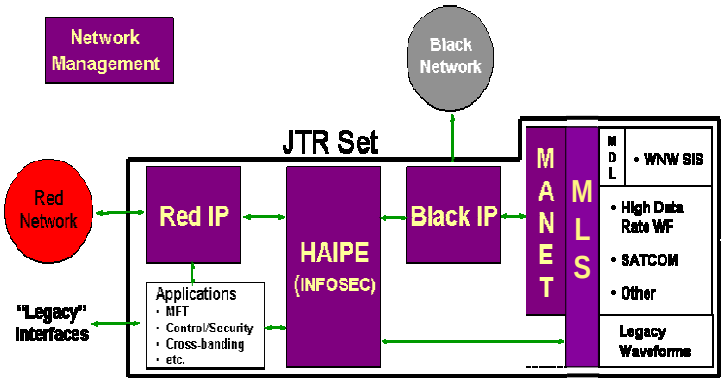


Figure 10: The Enhanced JTRS Architecture with Multiple Levels of Security Capability within the Networking Fabric

The current method that are employed for MLS is either the system operates in the clear (completely open) or operating entirely at the highest security level. Obviously operating in the clear is not a valid operating condition for secure operations. Operating at the highest security level prevents sharing information and segregates lower classifications nodes from the network. This is obviously not a desirable condition since it defeats the purpose of having a network. Therefore the use of physical isolation mechanisms or manual downgrading processing limits the utility of NCW.

Therefore a significant challenge is to develop a mechanism that a platform (individual node or network) can securely run multiple classification levels and move data between them, easily adapting as technologies change. Software techniques that implement security policies are one possibility. As stated earlier, the challenge with those systems is the provability of their secure operations. Hardware techniques that implement a specific security policy are another possibility. Figure 11 illustrates these two techniques. A software approach on the left side uses trusted processor hardware with middleware software that is the interface between the hardware and the isolated software streams. The hardware approach on the right addresses the problem by creating verified hardware security policy modules that can be combined to provide MLS. The challenge is to create enough diversity in the secure hardware elements in order to implement a complex security policy.

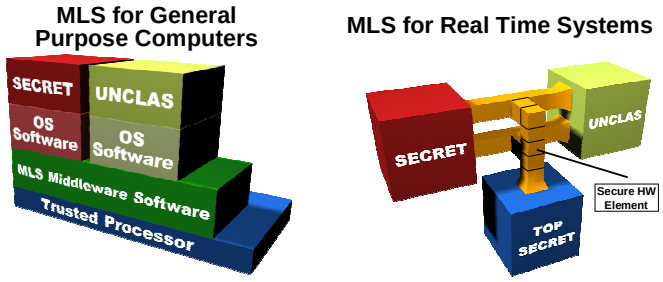


Figure 11: Software and Hardware Approaches for MLS

The security challenges that face mobile networking are immense. Mobility introduces increased vulnerabilities as well as a severe limit on the resources to address those vulnerabilities. In addition, the introduction unattended networked sensor

systems that can be tailored quickly to the specific mission places new emphasis on MLS techniques that address both intra-node and inter-node information security.

4. TECHNOLOGY NEEDS AND INITIATIVES

The promise of mobile networking is immense for both the commercial and military markets. Low power, resilient, ubiquitous networks enable new applications and capabilities. However, there are a series of hard problems within the networking, the radio efficiency, and security areas. Networking must be able to address the unique aspect of mobility with an RF environment. In particular, routing techniques are needed for changing topologies that are robust, scalable, and bandwidth efficient. The capacity to address the intermittent or interruptible behavior of RF links in a network. Also, there is a need for the development of intelligent gateways to enable multiple physical, network, and QoS instantiations for a network of networks architecture.

Due to the incompatibility between resource-rich wired networks and resource-poor wireless network, there needs to be significant technology development to improve communications efficiency. More efficient use of the spectrum, more efficient energy use for transmitted *information*, and efficient shared access to a satellite communications channel is needed. An additional area of radio efficiency is power, but with respect to the RF subsystem of a radio. There are still major shortfalls in wideband antennas, power amplifiers, and malleable pre- and post-select filters. These shortfalls impact energy efficiency as well as networking robustness.

The third area of additional technology needs is in security. Security for intra-node, multi-level security is needed for unattended sensors and relays. Communications security is needed to prevent intrusion into a mobile network. Advances in network security are needed that specifically address the limitations and potential advantages of mobile networks.

The technology needs listed above cannot be addressed by single techniques or the development of a new device. These problems need new insight into the problem space through both the understanding of the science (physics, communications, computation, and cyber) and the unique attributes of the problem space of mobile networking. Although much can be borrowed from the understanding of problems and solutions within other domains (e.g. the internet), new initiative must capture what is new and what is unique in our understanding and approach to mobile networking.

5. CONCLUSIONS

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-shooter-effector's linkages.

References

1. Interoperability: DoD's Efforts to Achieve Interoperability Among C3 Systems, GAO Report, April, 1987.

2. Conduct of the Persian Gulf War, Aspin Report, April 1992.

3. Joint Military Operations: DoD's Renewed Emphasis on Interoperability Is Important but Not Adequate, GAO Report, October, 1993.

4. DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," 09/19/2002.

5. Joint Tactical Radio System Wideband Network Waveform: Overview of GIG Wireless Network Vision, K. Schmidt, Milcom 2003 (find in www.afcea.org/pastevents/milcom2003/Schmidt_files).

6. Implementing the Global Information Grid (GIG): A Foundation for 2010 Net Centric Warfare (NCW), M. Frankel, DASD (C3ISR, Space & IT Programs), International Command and Control Research and Technology Symposium, June 2003, (find in www.dodccrp.org/events/2003/8th_ICCRTS/Pres/plenary/1_0915frankel.pdf).

7. Mobile Networking, D. Honey, DARPA, Briefing to R. Sega, Deputy Director for Research and Engineering – Office of the Secretary of Defense, November, 2004, (cleared for public release – Case 3613).

8. DARPA Connectionless Review, P. Marshall, personal communications, 2004.