World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:2, No:6, 2008

Improvements in Navy Data Networks and Tactical Communication Systems

Laurent Enel, and Franck Guillem

***Abstract*—**This paper considers the benefits gained by using an efficient quality of service management such as DiffServ technique to improve the performance of military communications. Low delay and no blockage must be achieved especially for real time tactical data. All traffic flows generated by different applications do not need same bandwidth, same latency, same error ratio and this scalable technique of packet management based on priority levels is analysed. End to end architectures supporting various traffic flows and including low-bandwidth and high-delay HF or SHF military links as well as unprotected Internet sub domains are studied. A tuning of Diffserv parameters is proposed in accordance with different loads of various traffic and different operational situations.

***Keywords*—**Military data networks, Quality of service, Tactical systems.

I. Introduction

FOR already many years military navy communications have been following their commercial counterparts concerning networks components (onboard Cisco routers, ip protocol stack …). They are now facing some of their problems : the amount of information continuously increases, the requirements of these data, regarding to the networks, are as various as the onboard applications generating these data (real time access to ground based data bases, voice and video communications, remote maintenance, sensor data exchanges between ships and from ship to shore …)[1] [2].

Depending on the tactical situation and the capacity of the networks, some application is of course more critical than others. The network is not always able to provide a guaranteed throughput and no jitter (isochronism) to voice and video communications, low latency (no queuing delay) to real time applications and zero errors to heavy data files transfers. To share at the best the capacity of the network between onboard applications throughout a priority mechanism is so a real progress to enhance navy communications performances and capabilities.

From source to destination data packets are transmitted on many different network links. Some of them are made of military and customary techniques and protocols. Onboard, the reasons why are numerous : need for a real time bus (fit for combat system data), difficulties to upgrade older systems, low bandwidth on HF links, latency on SHF channels [3], low emission needs to insure magnetic discretion …).

L. Enel is with Université du Sud Toulon Var, lab PPF STIC/TD, Institut des Sciences de l'Ingénieur de Toulon et du Var, BP 56 – 83162 La Valette Cedex France (e-mail: enel@univ-tln.fr).

F. Guillem is with Centre Technique des Systèmes Navals, Délégation Générale pour l'Armement, BP 28 – 83800 Toulon Naval (e-mail: Franck.guillem@dga.defense.gouv.fr).

Of course proprietary approaches are always less protocol stack compliant and specific application less interoperable. However newer combat systems are now evolving and have to exchange some of their data with other units (ships, planes, UAV) [4] or with ground based data treatment centres. These data are now coming to ip formatting (even if transmitted through link 11) [5]) and ip QoS management becomes a real need as over-provisioning is no longer financially and technically affordable. Data processing and routing should look like Fig. 1.

To improve navy networks capabilities it is possible to introduce internal priorities between military data using Diffserv AF PHB inside military domains. To improve reliability, it is also possible to take advantage from a multipath routing through Internet non military domains. The first point is quite obvious as bottlenecks are possible on RF or satellite links and critical data need to be prioritised .

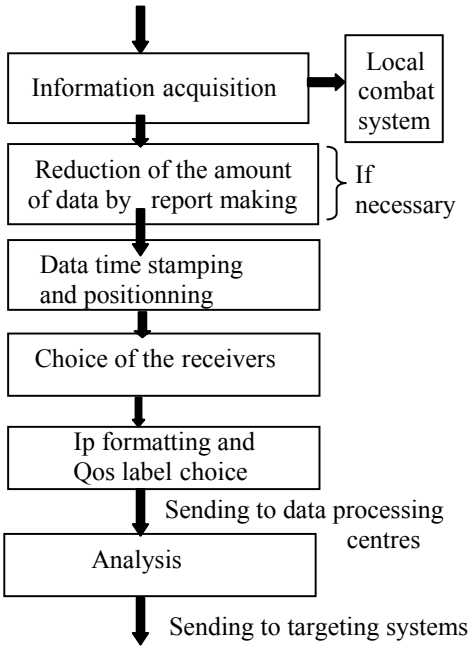

Fig. 1 Data routing and processing (embedded and ground based sensors)

The second point comes from the need to maintain the ability to send data even if the environment is partially destroyed. No absolute security can be insured on Internet even if, when there is a strong need to protect the privacy of the transmitted data, cryptographic techniques mixed with adapted key distribution, key management and ad'hoc

protocols are especially designed to meet accurate security. But some kind of data such as sensor data may take benefit of the internet meshing and of its quite perfect survivability, keeping in mind that unfiltered data from sensors are only vulnerable to modification.

Thus, information loss is not really a major problem: a track will not be refreshed, perhaps will be decorrelated regarding to track following made by other ships but will not be lost and will continue because of data availability from these other units. As well, replay is not dangerous because of the short time to live of data which have to be time stamped by the sender.

At last, the capture of rough data is not of any interest. As previously said, the only vulnerability stands when a change is furtively introduced in a message but this is a very complex operation because it would need to know how to modify data in real time so that it become false but believable [6].

II. Extended Combat System Architecture

At the beginning onboard naval combat systems were just one piece among many other systems belonging to one platform. This characteristic has been continuously evolving.

The combat system architecture has integrated first a cooperative engagement capability (CEC) [7]. This capability allows all the ships participating to a same naval force to share their detection capabilities (up to sharing unfiltered information issued from sensors) so that the naval force become a single distributed ship.

At this time combat system comes to a system of systems [8]. Sensors can be distributed between UAM, aircrafts, ships and shore based locations (mobile or not).

Thus, correlated information, after accurate processing inside centres of command, will allow to identify then destroy real targets thanks to as well distributed weapons systems.

Combat systems have been onboard for twenty years but the concept is now evolving and combat systems are no longer autonomous real time systems needing particular buses coming from GAM-T 103 standard.

To find an alternative to these buses is necessary to migrate somewhere tactical messages toward ip data formatting [5] but to insure equivalent performances will need efficient QoS management on any of the four kinds of domains described in Fig. 2 and Fig. 3.

A good end to end QoS will be based upon addition of improved QoS upon each of these different links and solutions wont be the same.

Combat system concept comes to be extended by an appropriate architecture operating with civilian internet links: for example littoral sensors linked trough internet to a whole system is able to protect a littoral city or area.

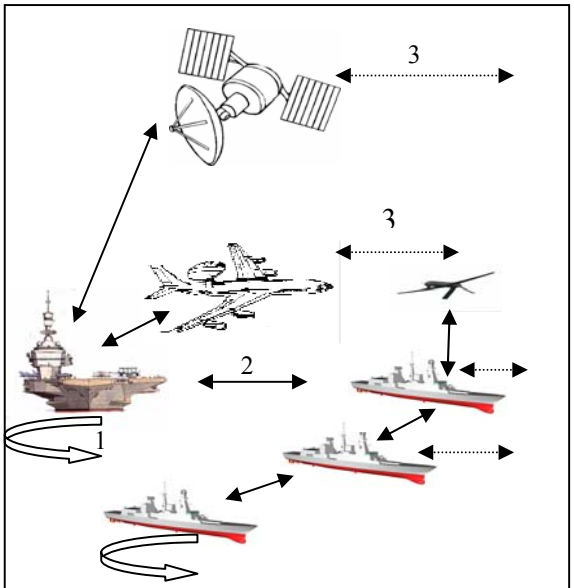

Fig. 2 Embedded part of the network

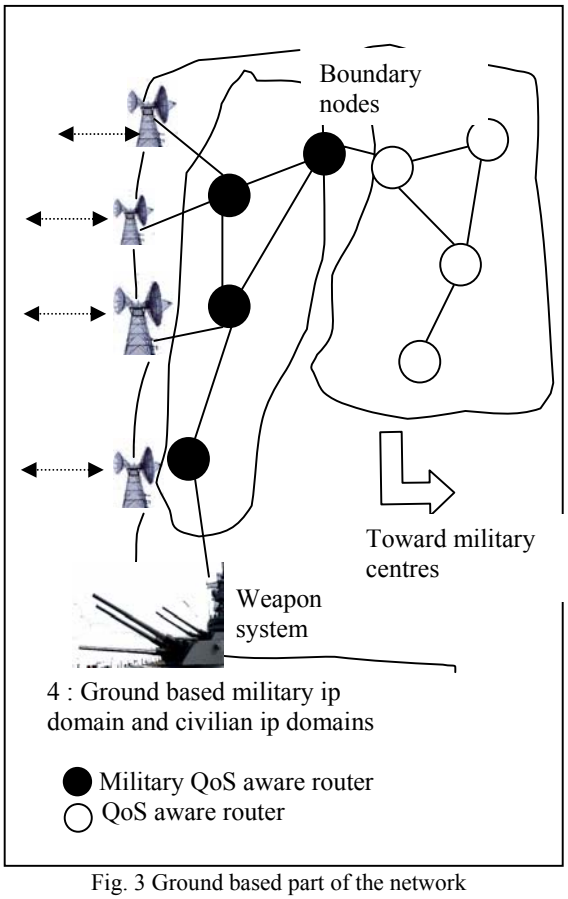

Fig. 3 Ground based part of the network

Despite of noticeable improvements in HF and SHF channel abilities, so that ip data can now be send over [9], the problem of ship to ship and ship to shore channel capability improvement still remains (according to an extended concept data need to be received on shore then send to ground based tactical host terminals and processors).

An ip formatting as close as possible to the data sources is very important (to get accurate time stamps and geographical GPS like stamps) but speaking of layer four, using TCP is not really possible upon ship to ship and ship to shore links [10].

So it is very illusory at this time to look for an end to end quality of service in a sense where an unique civilian quality of service management protocol would be used.

Between onboard sensor and the last ground based processor, information will have crossed many heterogeneous domains using their own techniques (onboard network, wireless military networks (link16, HF links…).

Upon military links we are not (speaking about sensor data) in a best effort context and all is done so that latency, allowed bandwidth are as good as possible. The way of improvement of quality of service management is to come from ground based civilian links transmitting military data.

Link 1 has already been studied and good solutions, sometimes even partly civilian, exists [11].

Links 2 and 3 will stay military because it is necessary to lower susceptibility to countermeasures by shutting down any radiation (thus duplex protocols are not welcome).

On segment 4, sensor data needs are close to civilian data needs such as real time video data or remote control data. Requirements on latency, isochronisms, burstiness, time to live, error rates …are encountered according to this or this sensor.

The problem is even more difficult if the number of military applications with their own platforms, full range speed requirements and geographical dispersion is taken into account:

- errors on platform positions are possible,
- some links may have very low bandwidth,
- latency is very different according to the link (HF, SHF…)
- complete diffusions of all data to any participant is impossible (While it can be achieved within smaller size Cooperative Engagement Capability concept).

The challenge is to choose and adapt, between all quality of service protocol families, the best ones, which will be suited for extended combat system concept.

III. QoS Management

Three main techniques can insure quality of service over ip networks: RTP/RTCP, Diffserv and IntServ. In the following is exposed what make think that DiffServ solution is certainly the best solution in this case.

First RTP itself does not provide all the level four transport protocol functionalities and usually works with UDP which can be a problem (reliability and security). RTP neither manages capacity reservation nor guarantees Qos or even priorities for real time services: RSVP is needed. RTP is just a frame of protocol , it is not complete and many other protocols must be implemented in complement to lead to a whole protocol stack fitting exactly an application needs (a session management protocol for example).

At last the heavy RTP/UDP/RTCP/RSVP full stack of protocols is much better adapted to local multimedia n to n conferences. The whole stack generates an important overhead and a significant management traffic load [12] and our needs must take into account n to 1 streams and also include non isochronous data.

Concerning the IntServ approach, each stream QoS characteristics must be memorised into any router of the IP domain. A data stream is made of following messages which have both same origin, destination and QoS requirements. Any stream gets a “flowspec” which is send to the network so that the network is able to reserve the right “resource”. To do so, RSVP protocol is used. It is of course necessary that application software knows how to specify its QoS needs according to the RSVP protocol and these requirements must be understood by any router crossed by the reservation request. If one single router is not OK the reservation fails over the whole way.

With regards to the combat system it would be thus necessary that:

- sensor data merge in some points of concentration which would dangerously lowers reliability (This to limit the total number of managed data flows), these points being able to manage RSVP;
- the routing of data from these points towards processing centres takes place through an homogeneous IntServ (civilian or military) domain.

Fig. 4 shows what could be an architecture without QoS management to compare with Fig. 5 showing an IntServ architecture.

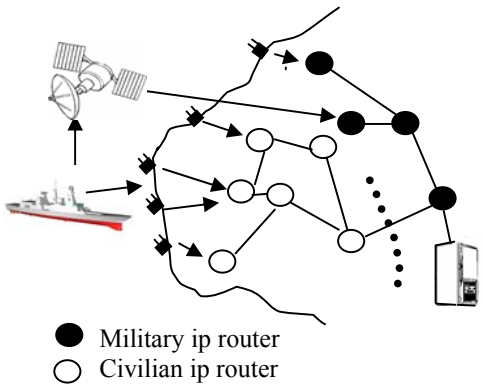

Fig. 4 Architecture without QoS management

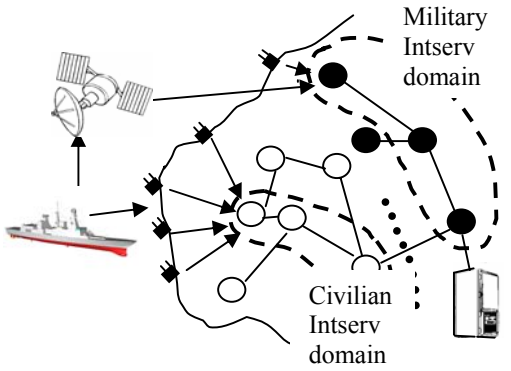

Fig. 5 Architecture with Intserv QoS management

IV. Data Classification and Codepoints Value

DiffServ technique [13] is more simple to set up but doesn't guarantee end to end QoS. It consists in giving a priority to ip datagrams which will be processed by routers according to this relative priority. This priority can be tagged by the source elsewhere in an unused field of the datagram. The diffserv ingress router will translate this priority into a diffserv priority tagged in the DSCP (diffenrenciated services codepoint) field of the ip header. Fig. 6 shows a possible DiffServ architecture.

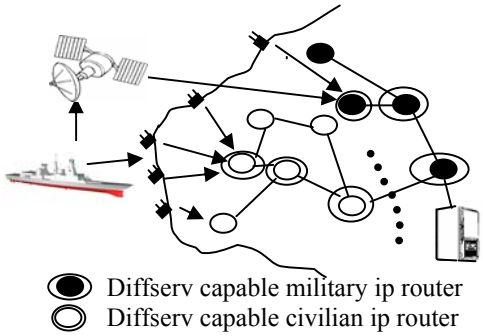

Fig. 6 Architecture with Diffserv QoS management

According to [13] the following values of the DSCP field are proposed to fit the extended combat system requirements:

- Using the PHB (Per Hop Behaviour) EF (Expedite Forwarding) could be useful within a civilian Diffserv domain. This value would give priority to tactical data over any other data.
- Using the PHB AF could be useful to introduce relative priority beyond tactical datas within a military DiffServ domain. Twelve relative levels of priority can be coded with the six bits long DSCP field.

Table II gives a proposal for a DSCP values management according to various types of traffic requirements (see Table I).

There are different ways to proceed so that data streams demanding the same quality of service are joined together to allow the data network to give them the right service. The amount of data produced is not the only parameter to consider. Even if for example different classes of radar sensors create variable data rate loads. Non-synthetic aperture radars generate highly pre-processed pictures.

The information data rate is heavily reduced by simply expediting reports of hits of automatic target recognition (if sampling at a particular dwell finds no potential target, nothing is reported). A report will consist of bytes which describe the target location parameters (bearing, range …): 640 bits should be enough. If we consider that such radars can encounter up to 2000 targets on a single scan, a 200kbits/s bandwidth may be all right. At the opposite, synthetic aperture radars generate data which will need very high bandwidth capability because for every pixel of the image, data are send without exception: the bandwidth requirement should be about 25 Mbits/s. Electro-optical cameras imply quite equivalent data rate loads.

Data stream classification can be achieved according to the maximum latency time allowed: a first group would involve sensors which can be dedicated to a single weapon (for example gun control radars) and a second group, those which are dedicated to search and imaging. The first group rather asks for latency time under one second whereas the second group asks for latency times between several second or even minutes.

TABLE I
Traffic Requirements

Traffic type	latency	badwidth	reliability
Raw data	Very low	high	Very high
Video	moderate	high	moderate
Tactical picture	moderate	moderate	moderate
Weapon control	low	low	Very high
Command control	high	low	high

TABLE II
DSCP Assignment Proposal

Traffic type	PHB/DSCP Into civilian domains	PHB/DSCP into military domains
Raw data	EF/101110	AF11/001010
Video	EF/101110	AF21/010010
Tactical picture	EF/101110	AF13/001110
Weapon controm	EF/101110	AF12/001100
Command control	EF/101110	AF23/010110

To be correlated sensor data will also need to be time stamped (when created) and localized. The timestamp option natively belonging to ip datagram should be useful but as each router crossed by the datagram can add its own - unuseful - timestamp and thus the overhead increases. A proprietary solution according to timestamping shoul has to be studied (timestamp written into the payload itself).

In the same way geopositioning which is not an ip option will also have to be written into the payload (two bytes should be enough).

V. Conclusion

This paper presents a new extended concept of naval combat system which leads to get a better interoperability between systems mainly using internet protocols and internet itself

The goal is to share and receive relevant data in real time, when possible, so that survivability, responsiveness and efficiency can be improved.

To have access to a same situational awareness will only be possible through an unique integrated data network and standardized protocols.

It is all the more true if useless human interfaces become useless and cumbersome and are short-circuited by an increasing number of direct and quicker machine to machine communications [14].

In certain cases the development of intermediary protocols (overlay protocols) will be necessary to limit the amount of data. It is already true concerning the updating of common operational pictures with protocols close to classical P2P protocols [15][l6].

Anyway, command and control, based on sensor inputs, as close as possible to real time will have to deal with quality of service management protocols.

As sensors are becoming miniaturized, high resolution, cost-effective, consequently embedded in satellite, UAV, ground vehicles and thus more and more numerous it is necessary to sort, make synthesis and give priorities amounts of data via QoS management as long as bandwidth, data processing and computing capabilities are not infinite. However, a special attention will have to be paid to avoid network-centric architecture intrinsic weakness (potentially vulnerable to one single failure, virus or type of attack).

References

[1] Marek Kwiatkowski, “a concept of differentiated services architecture supporting military oriented quality of service”, journal of telecommunications and information technology, fev 2003.

[2] L. Enel, F. X. Arques, “Embedded secured networks simulation”, *IEEE/IMACS Multiconference on Computational Engineering in Systems Applications* (CESA’03), Lille, 9-11 Juillet 2003.

[3] Glenn A. Briceno, D. J. Shyy, Jinglin Wu, “A study of TCP performance for mobile Satcom system over blocking conditions” , IEEE milcom’03, oct 2003.

[4] D.A. Barsaleau, M. Tummala, “Testing of Diffserv parformance over a U.S. navy satellite communication network”, *IEEE Milcom’04*, 2004.

[5] Ch. Alspaugh, A.K. Legaspi, “A violation of order: IP-QoS for tactical traffic”, *IEEE Milcom’02*, 2002.

[6] L. Enel, L. Martinet, “Caractérisation de flux et qualité de service pour systèmes de combat futurs”, *Annales des télécommunications*, N°7-8 vol 60, 2005.

[7] J. Hopkins, “The Cooperative Engagement Capability”, *Apl. Technical Digest*, Volume 16, Number 4, 1995.

[8] D.C. Schmidt and al, “Towards adaptive and reflective middleware for network-centric combat systems”, *CrossTalk*, Novembre 2001.

[9] D. G. Kallgreen, J. G. Smaal, “IP unicast/multicast operation over stanag 5066”, *IEEE Milcom’01*, oct 2001.

[10] Committee on Network-Centric Naval Forces, Naval Studies Board, National Research Council, Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities, *The national academies press*, 2000.

[11] L. Enel, F. Guillem, “Application of ATM Network Techniques to New Naval Combat Systems”, IEEE/*ICTTA’04*, Damas, 04/2004.

[12] D. Grossman, “New Terminology and Clarifications for DiffServ”, *Request for Comment (RFC)*, N°3260, 2002.

[13] H. Schulzrinne and al, “RTP: A Transport Protocol for Real-Time Applications” , *Request For Comment (RFC)* , N°3550, 2003.

[14] P. C. Nolin, “Pursuing Interoperability: The Need for Transatlantic Technological Cohesion”, NATO 2006 spring session committee report 071 STC 06 E, 2006.

[15] Li Li, Louise Lamont, “Support real-time interactive session applications over a tactical mobile ad hoc network”, IEEE milcom’05, Oct 2005.

[16] Wenjing Lou, Wei Liu, Yuguang Fang, “Spread: improving network security by multipath routing”, IEEE milcom’03, Oct 2003.