FFI RAPPORT

PERFORMANCE TESTING OF STANAG 4406 (MILITARY MESSAGING) USING IP OVER HF

JODALEN Vivianne, SOLBERG Bjørn, GRØNNERUD Ove,
LEERE Anton

FFI/RAPPORT-2005/01183

PERFORMANCE TESTING OF STANAG 4406 (MILITARY MESSAGING) USING IP OVER HF

JODALEN Vivianne, SOLBERG Bjørn, GRØNNERUD Ove, LEERE Anton

FFI/RAPPORT-2005/01183

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
P O Box 25, NO-2027 Kjeller, Norway

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
N0-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER FFI/RAPPORT-2005/01183	**2) SECURITY CLASSIFICATION** UNCLASSIFIED	**3) NUMBER OF PAGES** 61
1a) PROJECT REFERENCE FFI-II/822/110	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE** -	

4) TITLE

PERFORMANCE TESTING OF STANAG 4406 (MILITARY MESSAGING) USING IP OVER HF

5) NAMES OF AUTHOR(S) IN FULL (surname first)

JODALEN Vivianne, SOLBERG Bjørn, GRØNNERUD Ove, LEERE Anton

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

	IN ENGLISH:		**IN NORWEGIAN:**
a)	IP over HF	**a)**	IP over HF
b)	STANAG 4406 Annex E	**b)**	STANAG 4406 Annex E
c)	STANAG 4538	**c)**	STANAG 4538
d)	STANAG 5066	**d)**	STANAG 5066
e)	RF-5800H	**e)**	RF-5800H

THESAURUS REFERENCE:

8) ABSTRACT

This report is the final summary of a test activity of Project 822 SIGVAT HF. The STANAG 4406 (Military Messaging) and its tactical protocol profile has been tested over an HF link supporting IP. The automated HF technologies include the STANAG 4538 (3G HF), STANAG 5066 (2G HF) and HDL+, a data link protocol proposed for standardization. The work has been published in four international papers that are included as appendices in this report. This report references the papers, and add some results that have not been published. By using the S4406 Annex E protocol profile we have shown that a reliable message transfer is possible over an IP network which comprise an HF link. This opens for an architecture where the HF links may be directly utilized also for IP traffic from various other applications. Application Throughputs up to a few kilobits per second were achieved in our tests. However, an HF link will represent a potential "bottleneck" in an IP network and it requires special attention for optimum performance.

9) DATE 2005-04-26	**AUTHORIZED BY** This page only Vidar S. Andersen	**POSITION** Director

ISBN 82-464-0939-5

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

CONTENTS

Page

1 INTRODUCTION 7

2 PROTOCOL STACK OF STANAG 4406 USING IP OVER HF 8

3 IP OVER HF 8

4 CONGESTION CONTROL ASPECTS 9

5 MEASUREMENTS OF THROUGHPUT 9
5.1 The RF-5800H and its IP implementation of S4538 10
5.2 Comparison of the performance of S4406 Annex C and Annex E 10
5.3 Throughput measurements on a point-to-point link in the lab 10
5.4 Throughput measurements on a point-to-point link over-the-air 10

6 IP MULTICAST 10

7 COMPARISON OF THE PERFORMANCE OF S4406 ANNEX E WITH A DEDICATED HF MESSAGING APPLICATION 11

8 PROPOSALS FOR IMPROVEMENT OF THE P-MUL PROTOCOL (ACP-142) 11

9 IMPLEMENTATION ISSUES 12

10 USING THE RF-5800H TOGETHER WITH BID-1650 12

11 MMHS AS AN INTEGRATOR BETWEEN DIFFERENT BEARER SYSTEMS 13

12 OPTIMUM OFFERED LOAD FROM THE MMHS TO THE RADIO 14

13 CONCLUSIONS 18

References 19

A APPENDIX : IP OVER HF AS A BEARER SERVICE FOR NATO FORMAL MESSAGES 20

B APPENDIX : MILITARY MESSAGING IN IP NETWORKS USING HF LINKS 26

C APPENDIX : ON-AIR TESTING AND COMPARISON OF 2G AND 3G HF 34

D APPENDIX : NATO MILITARY MESSAGING IN THE TACTICAL DOMAIN – PERFORMANCE ISSUES OF AN HF CHANNEL 45

PERFORMANCE TESTING OF STANAG 4406 (MILITARY MESSAGING) USING IP OVER HF

1 INTRODUCTION

In the two first years of Project 822 SIGVAT HF at FFI, a main activity was to test the new STANAG 4538 (3G HF) (1) over-the-air. This work was a joint effort between QinetiQ in the UK, TNO-Telecom in the NL and FFI, and it has been documented in (2). An expressed goal of this test activity was to test IP over the new STANAG. In 2003 we saw the potential of combining the ongoing work on Military Message Handling Systems in another FFI - project; Project 840 STAROS, with our HF work. Since our two STANAG 4538 radios, the Harris implementation in RF-5800H, have a direct IP interface, and the STANAG 4406 (3) on formal military messaging may use IP as the networking technology, we decided to do some functional testing when connecting the application with the HF bearer service. STANAG 4406 was therefore used as a tool for exploring the IP capabilities of the radio and thereby fulfilling one of the goals of the 3G HF testing.

The initial functional testing developed to become a more thorough performance testing, and various aspects of the IP capabilities of the radio have been assessed. We also expanded the HF systems testing by including the 2G HF technology represented by STANAG 5066 (4) and the enhanced 3G technology represented by the HDL+ data link protocol proposed for NATO standardization by Harris.

During the work we have had good support by a Technical Assistance Agreement between Harris Corporation and FFI. In particular, Eric Koski of Harris has been very helpful and provided us with insight into complex technologies of their radio. For the STANAG 4406 application we have used the Thales XOmail implementation, and we have also received very good and expedient support from Thales Trondheim. In return, the two companies have received some new viewpoints and “bug-reports” on their implementations.

The results of our two years of work have been presented in various forums; the NATO BLOS COMMS Ad-Hoq Working Group, our projects Prosjektråd, and at conferences. There exist four international papers on the subject, and they are included in this report in Appendix A to D, in chronological order. Instead of repeating the contents of the papers in this report, we will refer to the most appropriate paper for a description of the specific topic. Some new / not published results are described in separate sections of this report. The four papers are listed here and can be found in the following publications:

Appendix A: IP over HF as a Bearer Service for NATO Formal Messages,
IEE Conference Publication No 493, 9th International Conference on HF Radio Systems and Techniques, pp 19-24, Bath, UK, 2003

Appendix B: Military Messaging in IP Networks using HF Links, *IEEE Communications Magazine*, Vol 42, No 11, pp 98-104, Nov. 2004

Appendix C: On-air Testing and Comparison of 2G and 3G HF, *Nordic HF Conference Proceedings*, p 3.5.1, Fårø, Sweden, 2004

Appendix D: NATO Military Messaging in the Tactical Domain – performance issues of an HF channel, *RTO Symposium on Military Communications, Proceedings*, RTO-MP-IST-054, Rome, Italy, 2005

2 PROTOCOL STACK OF STANAG 4406 USING IP OVER HF

When connecting the S4406 application with IP over HF as the bearer service, the two complete protocol stacks (Annex C and Annex E) are shown in Figure 1. The best description of the S4406 application and the HF STANAG's can be found in the introductory sections of Appendix B.

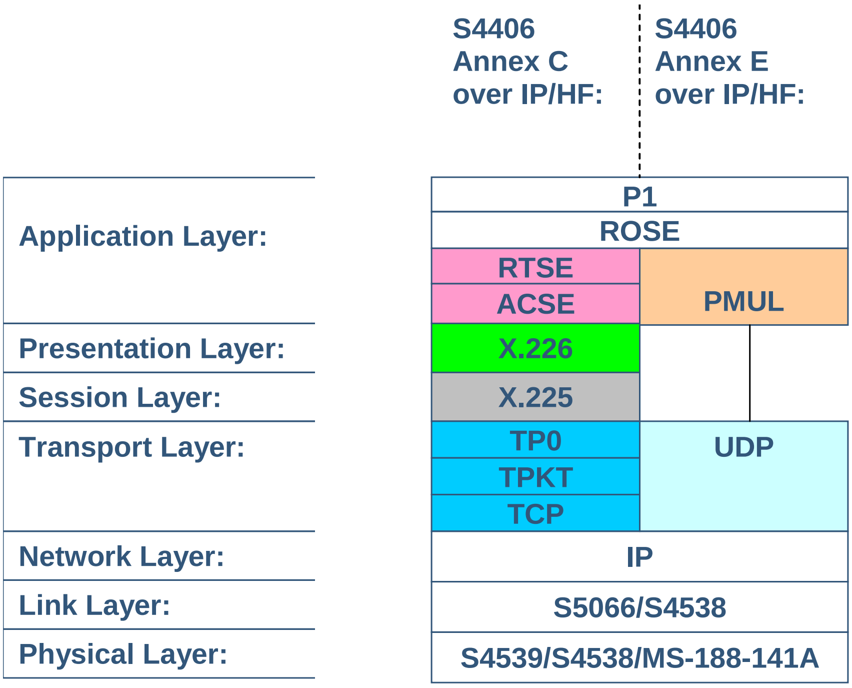

Figure 1 Protocol stack of MMHS (S4406) using IP over the various HF standards

3 IP OVER HF

A general description of a scenario where IP over HF is desirable and what the limitations are, is described in the introductory sections of Appendix B.

4 CONGESTION CONTROL ASPECTS

The lack of flow control/congestion control when the fast S4406 Annex E application is sending data packets to a slow HF radio is discussed in the section “Flow control aspects” in Appendix B. The shortcomings of the Source Quench technique and a proposal for a new congestion control mechanism are mentioned in section 6.1 of Appendix D.

Our experience with the RF-5800H and the firmware that we tested, was that a Source Quench packet was not sent from the radio until an overflow situation had occurred, and one packet had been discarded. This resulted in a NACK from the receiving application and a following retransmission. Harris has indicated that their implementation now sends a Source Quench packet *before* the overflow situation occurs, which will greatly improve the performance of the system, especially with respect to the vulnerability of P-Mul not receiving the last data packet of the message. We have not confirmed this new implementation of Source Quench.

5 MEASUREMENTS OF THROUGHPUT

We have used two definitions of throughput in our work. Most of our results are given as *Application throughput* which is the throughput experienced by the user of the messaging application when one message is sent at a time on a point-to-point link. It is defined in Figure 2. T_1 is the time when a message is sent from the message server, T_2 is the time when it is received by the receiving message server. At time T_3 the HF channel is released. *Data Link Throughput* is the true number of bits (including overhead) delivered by the HF service provider in a certain time period. Time for link setup is not included. We determined data link throughput by using an Ethernet “sniffer” counting transferred bytes and determining the transfer time from an oscilloscope on the HF channel. A formula for the relationship between application throughput and data link throughput is given at the end of section 7 in Appendix C.

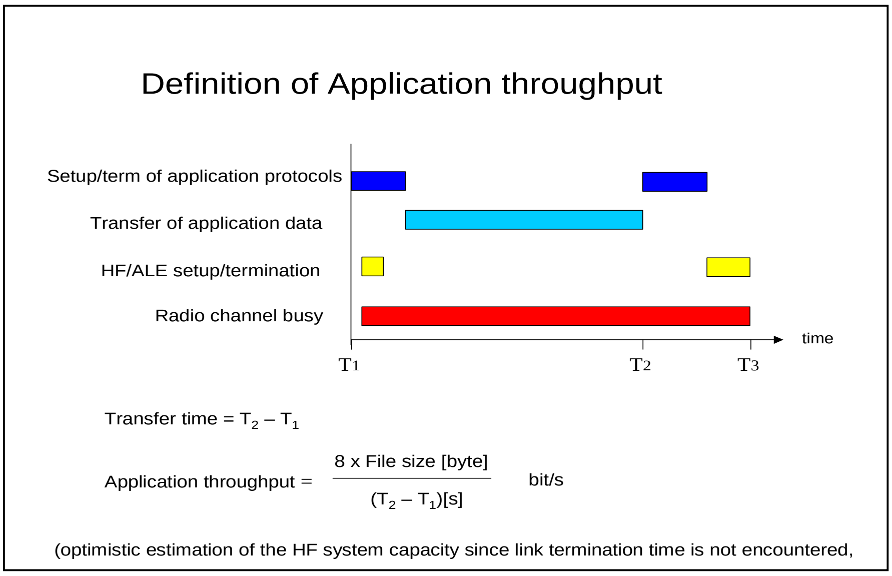

Figure 2 Definition of application throughput

5.1 The RF-5800H and its IP implementation of S4538

For IP traffic, the RF-5800H uses IP datagram concatenation and compression to enhance the throughput performance. This is discussed in Appendix A under “Throughput considerations and measurements”. An increased throughput efficiency is achieved by using these techniques, but this IP implementation will not necessarily be interoperable with other S4538 products, since these techniques have not been standardized. The NATO standardization group (BLOS COMMS AHWG) is now aware of this, and a standard for the IP interface is under development.

5.2 Comparison of the performance of S4406 Annex C and Annex E

Using the strategic, high data rate protocol profile defined in Annex C or the tactical protocol profile defined in Annex E over an HF link, is compared in Appendix A under “Throughput considerations”.

5.3 Throughput measurements on a point-to-point link in the lab

Our test setup in the lab is shown in a figure in section 7 of Appendix C for both the 2G and the 3G/HDL+ tests. The best description of these measurements is given in Appendix B under “Throughput Measurements”.

5.4 Throughput measurements on a point-to-point link over-the-air

A figure showing the test setup can be found in section 4.1 of Appendix D. The results are best described in section 7.2 of Appendix C.

6 IP MULTICAST

The lack of a standardized multicast packet data service in S4538 is pointed out in the “Multicast” section of Appendix A. This has been fed back to the NATO BLOS COMMS AHWG, and a proposal for a multicast protocol is now under development by the New Mexico State University.

However, the RF-5800H contains a non-standardized IP broadcasting service, on which a limited multicast service can be based. We have done some initial testing of the Multicast features of S4406 Annex E using this IP broadcasting service. This is described in Appendix D section 4.2. Using the broadcasting service of the RF-5800H, a fixed data rate has to be chosen in the radio. The data rate selected, is important for the probability of packet delivery. Figure 3 shows this probability of packet delivery versus SNR on the channel.

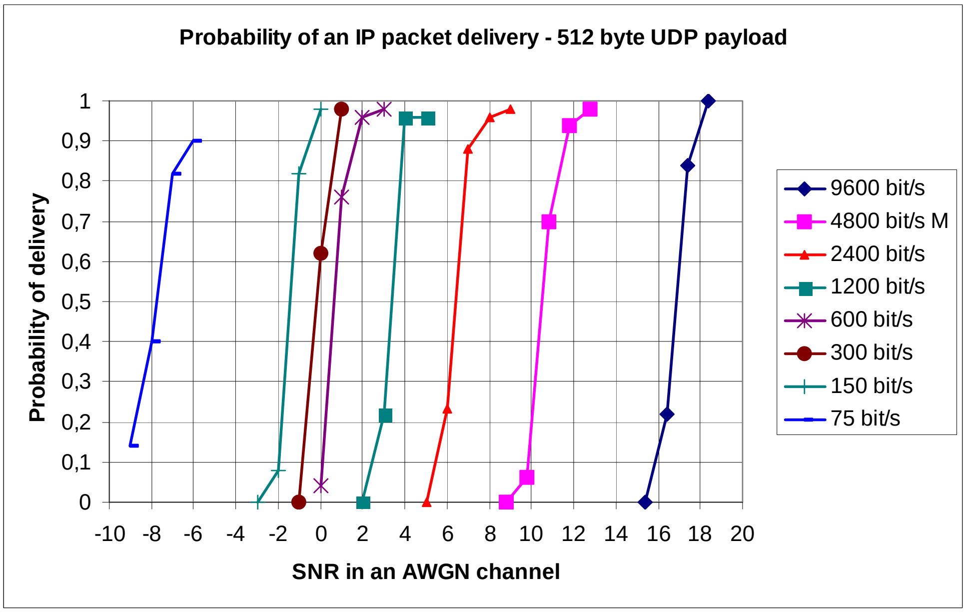

Figure 3 Probability of packet delivery for various data rates over a AWGN channel

7 COMPARISON OF THE PERFORMANCE OF S4406 ANNEX E WITH A DEDICATED HF MESSAGING APPLICATION

We here compare two applications used for completely different purposes, and the comparison may not be fair. We nevertheless thought it was interesting to quantify the penalty of introducing network functionality enabling an HF link to become an integrated part of the tactical internet. The dedicated HF messaging application is the Harris Wireless Messaging Terminal (WMT) using the Compressed File Transport Protocol (CFTP). The comparison is described in section 5.0 of Appendix D. A fair comparison between the two messaging applications could be possible if the subnetwork service interface of S5066 is used, and if a future version of XOmail would use the Service Access Point defined for S4406 messaging directly.

8 PROPOSALS FOR IMPROVEMENT OF THE P-MUL PROTOCOL (ACP-142)

Some shortcomings of the P-Mul protocol used in the S4406 Annex E profile have been identified, and are being worked on by NATO and the CCEB. Section 6.0 of Appendix D give an overview of the shortcomings and which solutions that will be proposed in edition 2.0. In addition to the proposals mentioned in Appendix D, pre-emption is also proposed in the new edition of P-Mul. This means that if P-Mul is processing a message, and a message of higher priority needs to be sent, the processing of the first message is temporarily stopped to allow immediate processing of the highest priority message.

9 IMPLEMENTATION ISSUES

We have noted several implementation choices that influence the performance that we have been measuring. Our results are only indicative of what can be obtained using these standards. We mention some of these implementation choices in section 5 of Appendix C.

During the period of testing, we have discovered a few “bugs” or shortcomings of the XOmail product. We have had a good dialogue with Thales Trondheim, and they have immediately provided us with patches that fixed the problems. According to Thales Trondheim, all the patches that we have received, have been incorporated in XOmail Version 11.3.

Similarly, we have had a dialogue with Harris Corp. We have received upgrades of the radio firmware along the way, and most of the tests have been conducted with a MP026 radio configuration. Their radio firmware V 1.3 and the WMT Version 6.0 should contain fixes to problems that we have discovered. FFI has not tried to confirm this.

10 USING THE RF-5800H TOGETHER WITH BID-1650

A Norwegian Army unit wanted to take part in the Cathode Emission Exercise in September 2004 with their newly procured Harris RF-5800H radios. A prerequisite for participation was *secure* e-mail. A way to achieve this, was to send Harris WMT messages using S5066, the BID 1650 crypto device and the internal modem (S4539) of the RF-5800H. The setup is shown in Figure 4. To achieve adaptive data rate, a crypto bypass solution for control signals was necessary, and this solution has been approved for use in military exercises by security authorities. Automatic Link Establishment (Mil-Std 188-141A) could also be used with this setup.

FFI was asked to find out whether the BID 1650 could be used together with the RF-5800H in this setup, and what we thought would be a two weeks job turned out to be a three months full time job for two persons. There were numerous problems, the three most important being:

- The clock signals from the radio were not compatible with the requirements of the BID 1650. Harris made a preliminary fix to this problem and provided us with new firmware in time for the Cathode Emission Exercise. This problem shall now have been permanently solved in the radio firmware version V 1.3.
- When operated together with the BID 1650, the S5066 protocol of the Harris WMT sometimes entered a “dead-lock” situation. This is now fixed in the WMT 6.0, but not verified by us.
- Independent of the use of the BID 1650, the S5066 introduced packet errors when run in non-ARQ mode. This is now also fixed in the WMT software, but not verified by us.

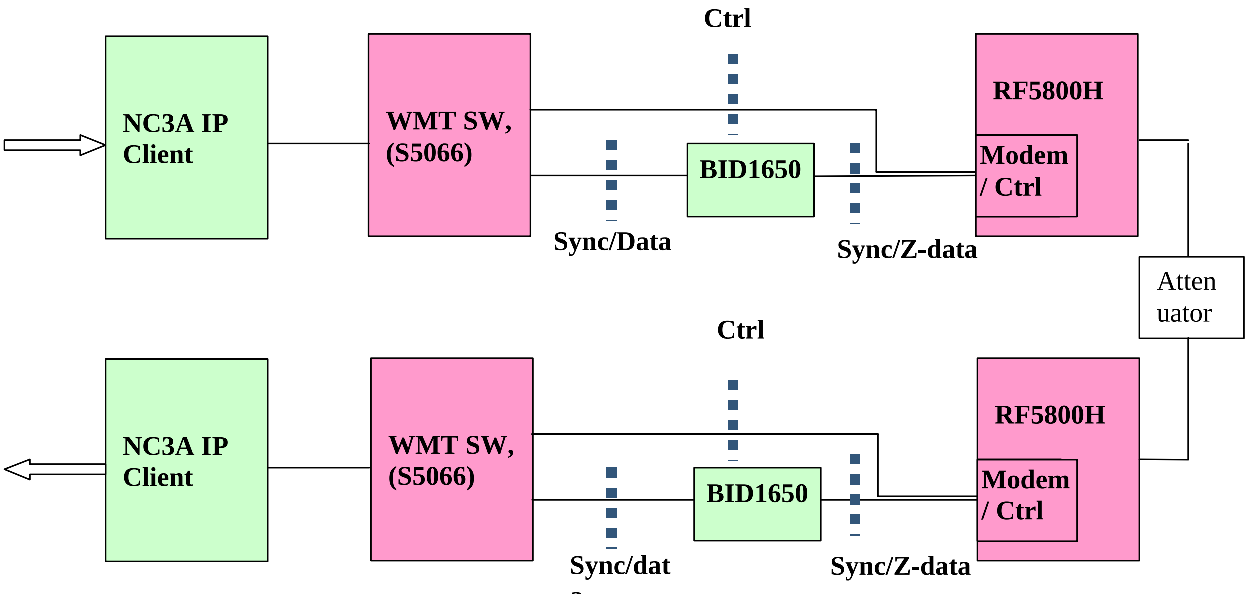

Figure 4 Set up for running S5066 with the external crypto BID 1650 and the RF-5800H

11 MMHS AS AN INTEGRATOR BETWEEN DIFFERENT BEARER SYSTEMS

The two protocol profiles of S4406, Annex C and Annex E, may provide a seemless interconnection between the strategic and tactical domain. The S4406 application may run over different networking technologies and bearer services. If IP is the networking technology of interest, and bearer services such as HF, UHF, etc are able to support IP, the S4406 application may “store and forward” messages over many hops using the underlying IP network. Static routes are defined in the various messaging servers. Since the work at SIGVAT HF also has included testing of the MMHS over the UHF radios IDM/MBITR (Thales)(5) and AN/PRC-117F (Harris)(6), we demonstrated the “store-and-forward” capabilities of the MMHS in a lab setup in November 2004. The demo setup is shown in Figure 5. The figure shows connectivity between an Army artillery battery and a Fast Patrol Boat Squadron (FPB Sq) deployed at sea and two Coastal Ranger Command Patrols (CRC) in the littoral environment. In the lab setup, the radios involved were the Multi Role Radio (VHF), the RF-5800H (2G and 3G HF) and the MBITR (UHF). Under ideal conditions in the lab, transmitting a 20 kbyte picture from the Artillery Batalion Headquarter to the Fast Patrol Boat Squadron and the Coastal Ranger Patrols took about 4-5 minutes.

The MMHS may also be used as an infrastructure for interconnection of other applications, by the use of a standardized Application Interface (API). In this way, the tactical protocol profile of Annex E may serve other applications as well.

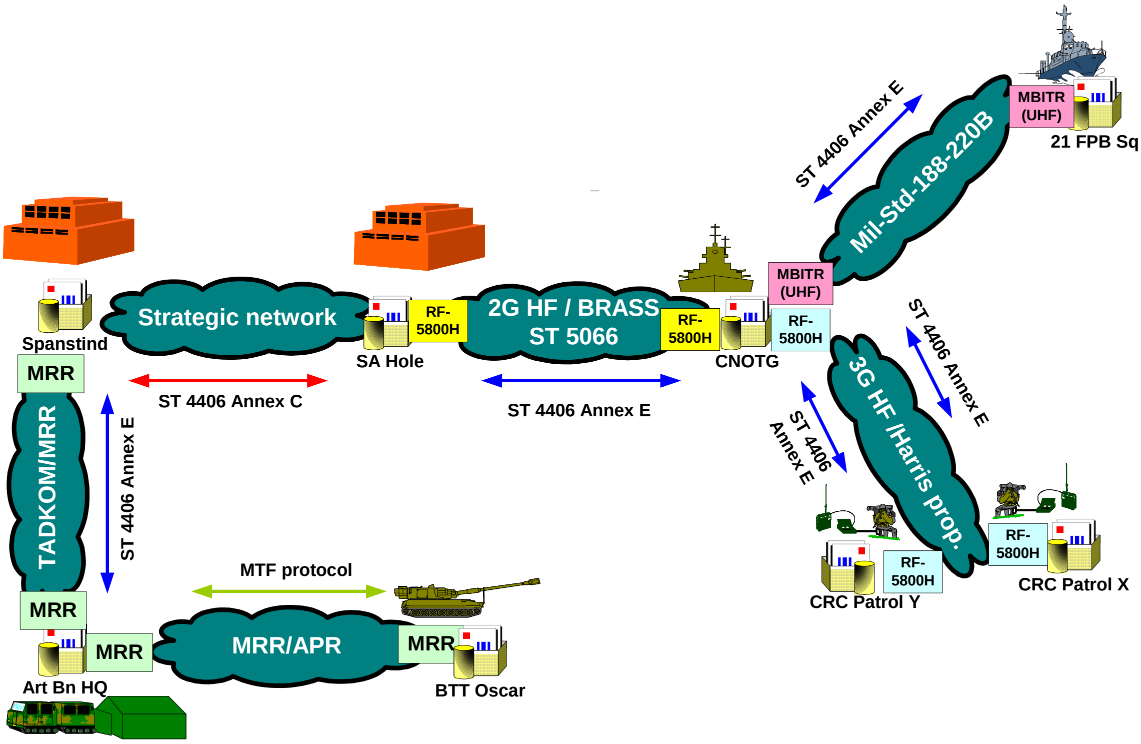

Figure 5 *Connectivity between Norwegian Land and Maritime forces using S4406 (MMHS)*

12 OPTIMUM OFFERED LOAD FROM THE MMHS TO THE RADIO

At the time being, in the spring of 2005 we have a Master student working on a conceptual topic related to the use of the MMHS. His work is not finished, so we will only refer what the topic is, and describe some initial results that are of interest to the user of XOmail over the RF-5800H.

The aim of this work is to explore two different concepts of transferring a message in an IP network where one or several links are tactical channels with varying quality. The first concept is shown in Figure 6, where the message server (S4406 Annex E) at Harris 1 is sending a message destined for Harris 4 via the message server at Harris 2. The three nodes are connected by two low rate HF channels (S4538) of variable capacity. The message server at Harris 2 receives the message, processes it and forwards it to the message server at Harris 4. A probably more realistic scenario would be that the two channels were in different frequency bands or representing two different HF systems.

The second concept is shown in Figure 7 where there is no message server at Harris 2, so the message sent from the message server at Harris 1 is routed directly by IP from Harris 2 to Harris 3 and further to the destination server at Harris 4. There is no possibility to influence the data rate over the IP connection from Harris 2 to Harris 3 in this concept. The report in (7) analyses the efficiency of the respective concepts in terms of throughput and how the channel conditions and parameter settings influence this efficiency.

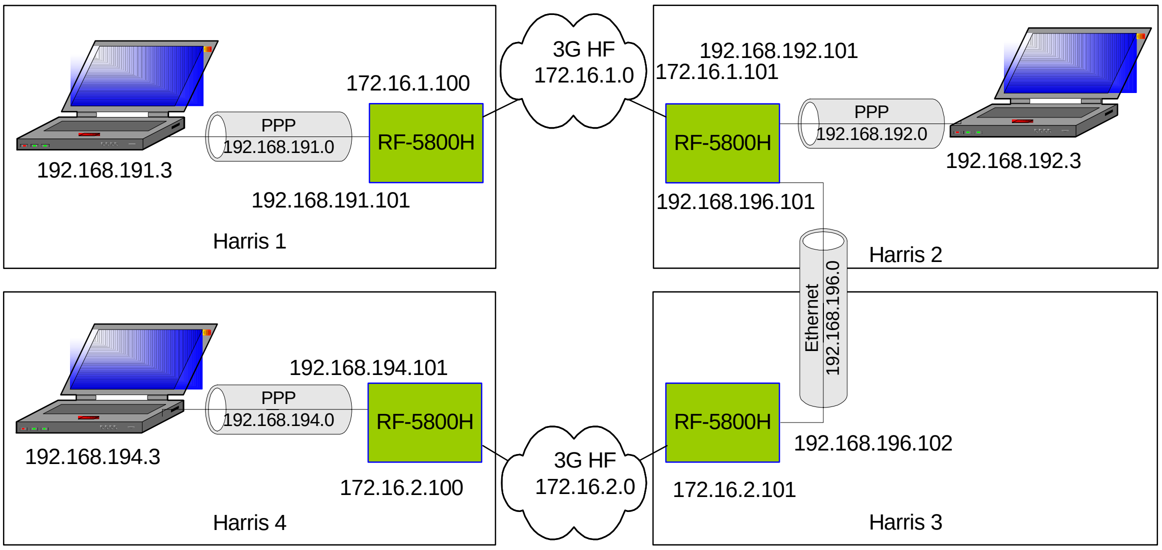

Figure 6 *Message transfer over two concatenated tactical links via a message server*

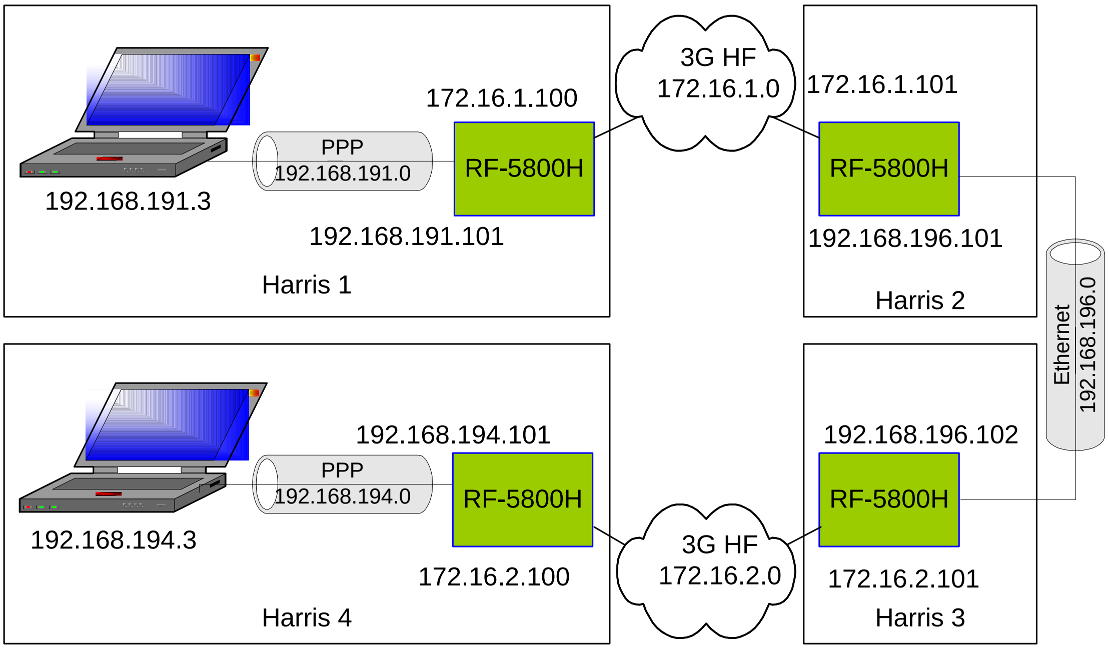

Figure 7 *Message transfer over two concatenated tactical links by direct IP routing*

Of more practical interest to the user of XOmail is the evaluation in (7) of parameter setting in XOmail for optimum performance over a single HF-link. For the published results reported earlier in this report, we selected the input data rate to the radio based on assumptions of “average” HF channel conditions and claimed that the results are *indicative* of what can be achieved. In (7) the interaction between the offered load, buffer handling and the data link protocol is analysed in more detail. Parameter setting for maximum throughput efficiency is a rather complicated task. Factors that influence this are:

- A relatively full buffer increases the throughput efficiency, and this is achieved by a high input data rate
- However, a high input data rate increases the probability of buffer overflow and Source Quench
- The HF channel conditions are variable so packets in the radio buffer are served at a rate that varies with time
- A Source Quench pauses the data flow from the sending P-Mul. The waiting time before transmission resumes can be configured in XOmail (Initial Delay) and the optimum value is dependant on the current available data rate on the channel
- Source Quench is associated with the loss of a packet in the firmware that we have tested. When the probability of Source Quench is increased, the probability of loosing the last PDU of the message (as well as other PDU's) also increases. In the current version of P-Mul, if the last PDU from P-Mul is lost, no NACK is generated from the receiving P-Mul, and a complete retransmission is triggered by a timer
- A complete retransmission based on the loss of the last PDU (all previous PDU's have been received) is very inefficient
- If a *small* value of the retransmission time-out is chosen, a retransmission may be triggered when message transfer is still in progress on the HF channel that is temporarily experiencing bad conditions and transferring data at a low rate

In (7) various PDU-delays and PDU-sizes have been tested and the application throughput results are shown in Figure 8 for an ideal channel (+40 dB). Five message sizes ranging from 400 bytes to 75 kbyte were tested, and the effect of Source Quench is included in the throughput values. Before giving some guidance on which parameter values to choose, we must point out the limitations to the analysis presented in (7):

- It is applicable only to this particular radio; RF-5800H.
- A unicast scenario only is analyzed.
- Only one traffic source is sending data packets to the radio.
- HDL+ has not been assessed, only HDL/LDL (HDL+ will most likely be used in real operations if it is available in the firmware).
- As we noted earlier in this report, if the Source Quench implementation has been changed in the radio firmware to issue a Source Quench *before* an overflow situation occurs, the results in (7) referenced here, will change.
- Some other parameter settings of the radio and application also influence the results. In (7) these parameters are explained a little more in detail. The values used in the tests are: Txprebufferdelay 1 s, Initial delay (after Source Quench) 20 s, Increased PDU delay (after Source Quench) 10%, Sustain period (before returning to initial PDU delay) 40 s.

- The measurements in Figure 8 were conducted using the Ethernet connection of the radio. Some differences were observed when using the PPP connection.

For a situation where all these conditions are applicable, we may give some rough guidelines on which PDU-size and PDU-delay that should be selected for *unicast traffic*. For best utilization of the buffer of the RF-5800H, a PDU-size of 1000-1472 bytes is recommended. *If no knowledge of the message sizes to be transmitted or the HF channel conditions exists, we recommend a PDU-size of 1024 bytes and a PDU delay of 850 ms.*

If message sizes are known to be small, below the radio buffer capacity of approximately 20 kbyte, the highest throughput efficiency is achieved by selecting a small PDU-delay, for instance in the 50-300 ms range. This will fill up the buffer rapidly with the whole message without exceeding the buffer capacity and without any Source Quench being sent out.

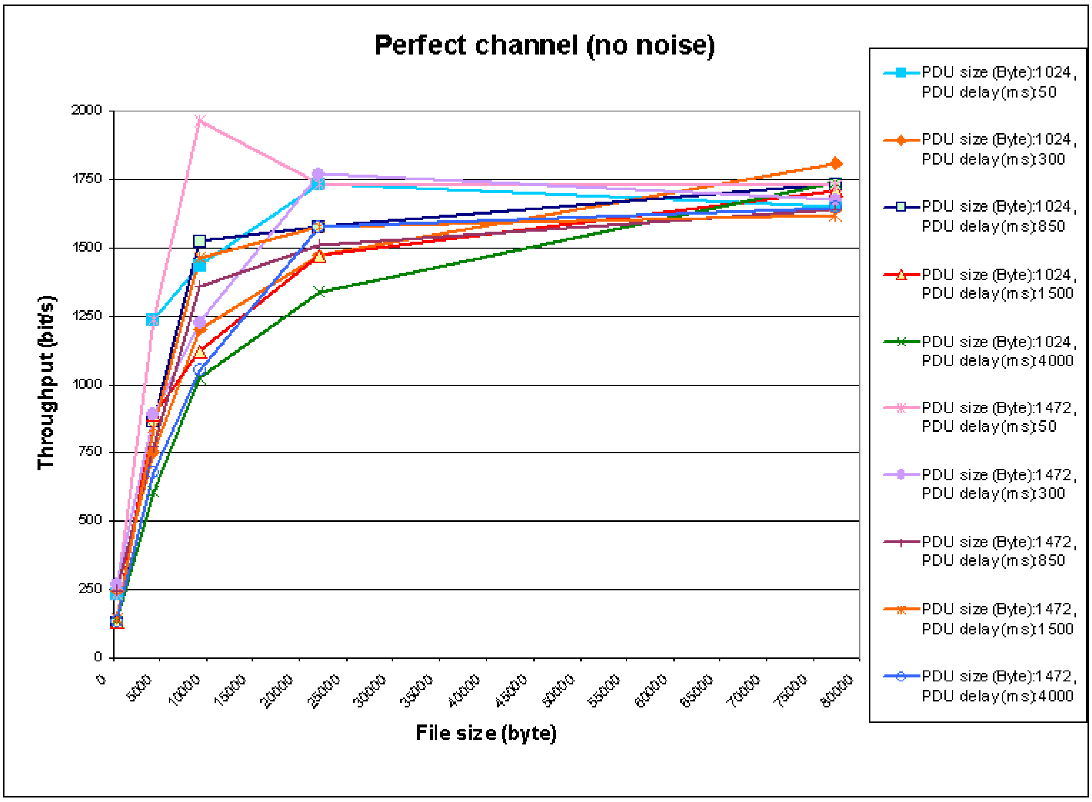

Figure 8 Application throughput vs message size for various combinations of PDU-delay and PDU-size under the conditions mentioned in the main text

13 CONCLUSIONS

The technical conclusions can be found at the end of the various papers in Appendix A to D. We conclude this report by a quotation:

... On 11 Sept when all the phones were out in New York City, we had 100% comms with our units and with our neighboring states through HF and your Fanlite antennas ... and we still do ...

WO Dave Tiffany
NY National Guard

HF .... it works !

References

(1) NATO Standardization Agreement (STANAG) 4538, Edition 1, Technical Standards for an Automatic Radio Control System (ARCS) for HF Communication Links

(2) Jodalen Vivianne, Grønnerud Ove, Testing of STANAG 4538 (3G HF) implemented in Harris RF-5800H, *FFI/Rapport-2005/01182, 2005*

(3) NATO Standardization Agreement (STANAG) 4406, Military Message Handling System (MMHS), Ed. 1, 1999

(4) NATO Standardization Agreement (STANAG) 5066, Profile for High Frequency (HF) Radio Data Communications, Version 1.2

(5) Solberg B, Grønnerud O, Overføring av IP meldingstrafikk over IDM/MBITR – resultater av lab testing, *FFI/Rapport-2005/01185,* 2005

(6) Jodalen V, Grønnerud O, Solberg B, Initial lab testing of IP messaging over the AN/PRC-117F, *FFI/Rapport-2005/01184,* 2005

(7) Simonsen Audun, Evaluation of message transfer on concatenated tactical links, *Master Thesis,* Norwegian University of Science and Technology, Faculty of information technology, mathematics and electrical engineering, Department of Telematics, 2005

A APPENDIX

IP OVER HF AS A BEARER SERVICE FOR NATO FORMAL MESSAGES

IP OVER HF AS A BEARER SERVICE FOR NATO FORMAL MESSAGES

V Jodalen, B Solberg, A Eggen, A B Leere, O K Grønnerud

Norwegian Defence Research Establishment, Norway

INTRODUCTION

A core element of Network-Centric Warfare is one common data network where all information is available to all authorized users. The introduction of IP services in all parts of the military networks will be an important contribution in this respect, providing a ubiquitous service to which applications may connect. This should apply even for low bandwidth transmission media such as the HF radio channel. However, for such channels the use of efficient communication and application protocols is essential. Interoperability between equipments and between nations requires the protocols to be standardized. During the last few years NATO has produced STANAGs for HF communications and efficient messaging. These will enable more unified data services between the HF network and other parts of the military network.

The HF NATO STANAG's 5066 and 4538 define protocols on the two lowest layers of the OSI model. STANAG 4538 (1) defines a subnetwork service interface that includes IP, and STANAG 5066 (2) defines a subnetwork service interface upon which IP services may be implemented. The use of either of these two STANAG's can provide a transparent IP service across the HF subnet, thereby including the HF subnet as part of the military IP network.

In NATO, Formal Military Messaging is standardized in STANAG 4406 (3). The recent Annex E of this STANAG defines protocols for efficient messaging over narrow bandwidth connections. This contributes to a seamless military messaging system, eliminating the need for special messaging gateways to communicate by HF or by other low bandwidth media. The Annex E protocols are based on using a connectionless communications service, such as IP unicast and IP multicast.

The aim of our study is to explore the use of STANAG 4406 Annex E on top of an HF radio subnet that offers an IP transfer service (STANAG 5066 and 4538). In this paper we have studied the interactions between protocols defined in STANAG's 4406 and in 4538, how they can interact in an optimum way with each other, and what the current limitations are. Protocols are described, and typical response times are measured in the lab on a perfect HF channel (no channel errors). Considerations regarding interoperability when running IP over HF are also given.

NATO STANAG 4538: ARCS

Several NATO STANAG's have emerged in the last decade. Most of them have a counterpart in the American Military Standards (Mil-Std). STANAG 4538 is a standard at physical and data link layer, and it represents the 3rd generation of automatic radio functionality, named ARCS (Automatic Radio Control System) in the NATO nomenclature. The main functionalities it describes are link setup (robust and fast), link maintenance, and the data link protocol named xDL which uses a set of four defined burst waveforms for packet data traffic. The standard supports analog and digital voice, in addition to circuit and packet-switched data.

The data link protocol xDL is defined for a point-to-point link, and it can further be divided into two classes of protocols called HDL (High throughput Data Link) and LDL (Low latency Data Link). HDL is optimized for delivering large datagrams in good channel conditions and LDL is optimized for delivering small datagrams in all channel conditions and also longer datagrams in poor channel conditions. The different performance of HDL and LDL under various channel conditions is caused by the characteristics of the different burst waveforms used. Both protocols employ Automatic Repeat Request (ARQ) and code combining for adaption of data rate to channel conditions. This has proven to be an efficient way of adapting the transmission to various channel conditions, Chamberlain et al (4). HDL and LDL exist in different variants, and a number n (eg HDLn) specifies the size of one forward transmission. For HDL the number n should be multiplied by 233 bytes to give the total number of bytes in one forward Tx frame. For LDL the number n gives the number of bytes explicitly. The largest forward Tx frame is 5590 bytes (HDL24). HDL employs selective retransmission of the packets. If the datagram is not filling up a forward Tx frame, zeros will be appended. Efficiency of the data link protocol is therefore dependant on the size of the datagram transmitted. For datagram sizes larger than ~ 250 bytes and perfect channel conditions, the HDL protocols will give best throughput. The theoretical throughput capability of the HDL protocols transmitting a datagram in one direction is given in Figure 1. Asymptotic throughput values (long datagram) for the LDL protocols are 126 bps for LDL32 and 486 bps for LDL512.

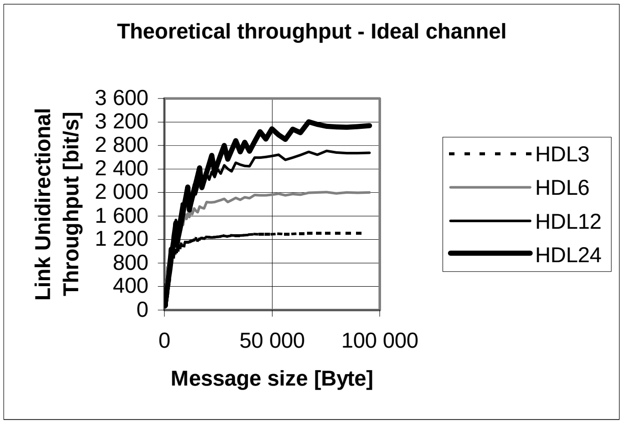

Figure 1: The potential throughput of HDL protocols. Ideal channel, no channel errors.

The xDL data link protocol is defined only for a point-to-point (unicast) link. STANAG 4538 also describes a synchronous two-way point-to-multipoint link setup where a number of units are addressed in a multicast call. Each of them responds sequentially, confirming that they can hear the caller. However, no point-to-multipoint packet switched data service is defined within the STANAG, only a circuit switched data service. Once the point-to-multipoint link has been established, only circuit switched data can be sent.

STANAG 4538 defines the subnetwork interface (to higher layers of the OSI-model) to be an IP interface. No further specification of the IP interface is given, since it does not affect over-the-air interoperability. Mil-Std-188-141B Appendix F (5) references the STANAG 5066 Annex A (Subnetwork Interface Sublayer) to be used, but STANAG 4538 has currently no references to this.

NATO STANAG 4406: FORMAL MILITARY MESSAGING

This section describes the application that has been run over STANAG 4538.

Formal messaging within the defence community has hitherto been based on the NATO ACP 127 Systems (6) for both strategic and tactical systems. The defence community is now migrating from ACP 127 to adopt military messaging products based on the STANAG 4406 Ed.1 military standard.

A Formal Military Message is different from an interpersonal message in that it is a message sent on behalf of an organization, and that it establishes a legal commitment on the part of that organization under military law. Examples of formal messages are military orders.

Formal Military Messages are handled by Military Message Handling Systems (MMHSs). An MMHS takes responsibility for the delivery, formal audit, archiving, numbering, release, emission, security and distribution of received formal messages. In NATO, the formal messaging service is seen as the vehicle for secure, mission critical, operational, military applications (e-mail systems are not).

STANAG 4406 Ed.1 is the only agreed standard to achieve interoperability between NATO nations' MMHS systems. Strategic systems compatible with STANAG 4406 have been and are being implemented widely by NATO and the NATO nations.

The connection-oriented protocol stack defined in STANAG 4406 Annex C for strategic high data-rate networks is not suitable for tactical low data-rate connections. The protocol solution in Annex E has therefore been developed as a replacement for ACP 127 systems in the tactical environment. With STANAG 4406 Annex E, a common baseline protocol solution exists that may be used between the strategic and tactical environments and within the tactical environments. Some of the characteristics of the STANAG 4406 Annex E are:

- interoperable with the NATO strategic MMHS systems (STANAG 4406 Annex C)
- opens for re-use of the MMHS applications from the strategic MMHS systems in the tactical systems
- increases the messaging throughput substantially for tactical communication channels with low data-rate compared to Annex C protocols
- connectionless
- may be used over full-duplex, half-duplex or simplex (broadcast) connections
- may be used for both multicast and unicast
- handles EMCON (radio silence) recipients

Figure 2 shows the layered architecture of the STANAG 4406 Annex E protocol profile. The profile is divided into an application layer and a transport layer on top of the potential bearer systems. The application layer is again divided into more specific sub-layers.

The messaging sub-layer is the same in Annex E and Annex C, in order to be able to use the same messaging applications. The service interface (TA-SAP in Annex E) is therefore the same whether the Annex C (connection oriented) or Annex E (connectionless) protocol profile is used.

The Tactical adaption sub-layer is "faking" the connection establishment and termination phases at the TA-SAP service interface in order for the applications to use the same service primitives whether the Annex C or the Annex E protocol profiles are used. In addition, this sub-layer performs compression and decompression of the whole message (both envelope and content).

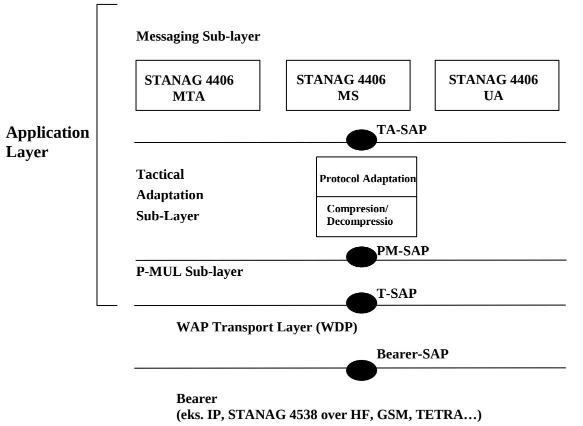

Figure 2: The STANAG 4406 Annex E protocol profile

The P-Mul sub-layer is defined by the military standard ACP 142 (7). This sub-layer has functionality for both multicasting and unicasting of messages. It splits the message into smaller Protocol Data Units (PDUs), attaches a checksum, numbers the PDUs and handles retransmissions based on a selective repeat procedure.

The WAP Transport Layer uses the connectionless Wireless Datagram Protocol (WDP). This protocol is more flexible than the UDP protocol in that it does not mandate the use of IP. If IP is used however, the WDP protocol becomes UDP. In our tests where the HF radio provides an IP service, UDP is used.

TEST SETUP FOR RUNNING THE APPLICATION OVER HF RADIO

A few vendors are now implementing STANAG 4538. The implementation of Harris Corporation is so far the most advanced, including for instance xDL, fast link setup and an IP service interface. Our lab tests have been run using two Harris RF-5800H man pack radios connected back-to-back. The Thales XOmail Server and Client software is an implementation of STANAG 4406 including Annex E. The test setup is shown in Figure 3, and it shows two Ethernet LANs where the mail client, server, and HF radio are connected. Each node has an IP address and the HF radio acts as an IP router to the Ethernet LAN on the other side.

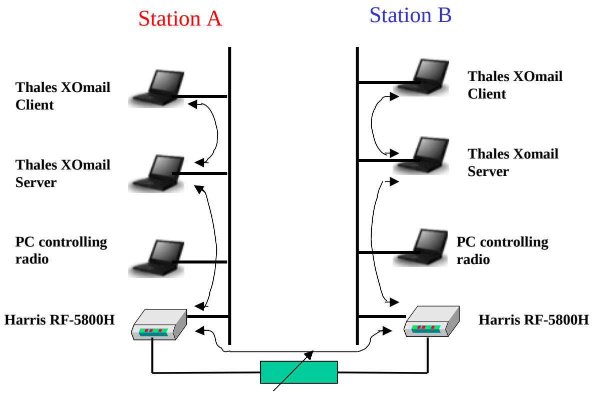

Figure 3: Test setup

To be able to examine protocol behaviour and packet flow in the test setup, two Ethernet "sniffers" and an oscilloscope have been included in the test setup. This is shown in Figure 4 together with the protocol stack in the mail servers (PC A and B). The P-Mul PDU size is a configurable parameter set to 512 bytes in the server software. The UDP/IP protocols add 28 bytes to the packet giving an IP PDU packet length of 540 bytes. The packet delivery rate from the mail server onto the Ethernet was set to 30 ms.

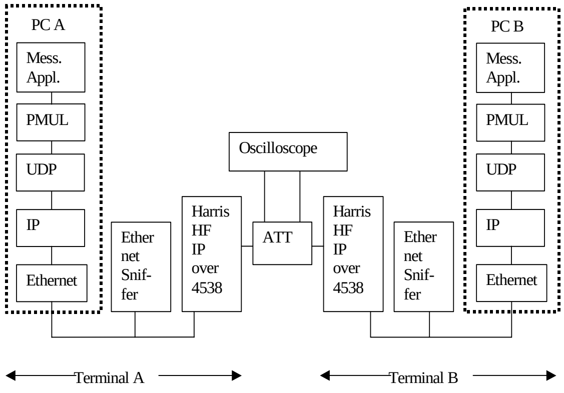

Figure 4: Test setup including protocol stack

OBSERVATIONS AND TEST RESULTS

Multicast

Future tactical data networks will be based on IP, and a multicast network service is expected to be available to the end users. Future HF radio networks will increasingly operate as part of an overall network. For ease of interoperability with the remaining parts of the network, the services offered by the HF network should be as compatible as possible with the services available in the Tactical Internet.

One of the main features of the P-Mul protocol in 4406 Annex E is its ability to offer a reliable multicast messaging service. Multicasting may be a bandwidth efficient way of transferring messages intended for several different destinations, provided that the underlying network also offers a multicast data transfer service. However, the multicast service offered by the network does not necessarily need to be reliable. An IP multicast service in the HF network is desired if full advantage of the P-Mul protocol shall be obtained.

The STANAG 4538 data link protocol does not presently define a point-to-multipoint packet data service or a broadcast data service. This prevents the use of the multicast features of P-Mul in STANAG 4538 subnets. Unless the STANAG 4538 is extended to cover for a point-to-multipoint packet data service, IP multicast traffic could be serviced in one of the following manners:

1. The STANAG 4538 subnet serves the IP multicast traffic by employing N unicast transfers rather than one multicast transfer per datagram. The xDL datalink protocols with their unique feature of adaptive data rate through code combining would then be utilized. The IP network will in this case perceive the HF network as giving a very slow, but very reliable transfer of multicast packets. However, the potential gain in efficiency offered by multicasting on a radio channel is lost.

2. The STANAG 4538 subnet serves the IP multicast traffic by setting up a circuit switched point-to-multipoint service, on which IP multicast datagrams are transferred using standard modems (e.g. STANAG 4539) and employing a suitable non-ARQ link protocol. This would, however, in effect represent an extension to STANAG 4538 since the latter, in contrast to STANAG 5066, does not define a broadcast link protocol. This approach presents a non-reliable packet transfer service to the user. This may be acceptable for the STANAG 4406 Annex E, since the P-Mul protocol rectifies this by applying an efficient acknowledgment and retransmission protocol. However, an adaptive data rate adjustment according to channel conditions will be more difficult using a non-ARQ link protocol compared to the unicast link protocols (xDL) of the STANAG 4538.

If the multicast capabilities of the STANAG 4406 Annex E are to be fully exploited in an IP network of which a future STANAG 4538 HF subnet is expected to be a part, the latter should be able to handle the IP multicast service. Moreover, the STANAG 4538 also lacks features for handling IP packet transfer to destinations in radio silence, which is another important capability of STANAG 4406 Annex E. This could be solved by a future definition of a non-ARQ packet link protocol to complement the existing STANAG 4538 link protocols and make the STANAG 4538 more applicable when serving protocols like STANAG 4406 Annex E in an IP environment.

Since STANAG 4538 does not define an IP multicast service, and the tested implementation of STANAG 4538 does not support multicasting, STANAG 4406 Annex E has been run in unicast mode in our lab tests and full utilization of the xDL data link protocols at HF has been made.

Flow control between the application and the radio

STANAG 4406 Annex E uses the connectionless transport protocol UDP when the network protocol is IP. UDP does not provide end-to-end flow control as TCP does. Neither does P-Mul have special protocol mechanisms for flow control, other than delivering PDU’s at a specified rate. Our application generates data at a much higher rate than the HF link can handle. Consequently, for large messages, congestion will occur in the HF radio, which will start discarding packets.

To reduce the effect of this congestion, some form of flow control of the P-Mul PDU’s should be introduced. This may be done by means of ICMP Source Quench packets. The Harris radio is capable of generating Source Quench packets, and the Thales 4406 Annex E software is capable of responding to these packets. However, discarding of packets in conjunction with the source quenching may lead to some reduction of the overall protocol efficiency.

For the ICMP Source Quench service to work properly, a minimum time interval between packets delivered by P-Mul should be set. This allows for processing time and routing of the ICMP Source Quench packet back to the data source.

Throughput considerations and measurements

The data link protocols of STANAG 4538 offer a reliable delivery of a datagram from the sender to the receiver. No presumption is made on the size of the datagram. A datagram could be constituted of one complete long message, or it could be a short IP packet. The efficiency of the data link protocol will, however, strongly depend on the size of the datagram, as pointed out earlier.

A message transferred by an IP network is normally comprised of many independent IP packets. A STANAG 4538 HF subnet operating as part of an IP infrastructure has to transfer each of these datagrams. However, when the STANAG 4538 handles the transfer of each IP packet independently, the efficiency of the link protocols decreases. Consequently, the throughput of the HF link may be substantially reduced compared to transferring the whole message as one datagram.

A simplified example will illustrate this degradation of throughput. Assume that a message shall be transferred from A to B. The STANAG 4406 Annex E protocol segments a message into UDP/IP packets with a maximum length of the IP packet of 1500 byte. If the length of the message to be transferred is 15 kbyte, a total of 11 IP consecutive packets are required for the message transfer. Consider now how the STANAG 4538 protocols operate when transferring one IP packet in the STANAG 4538 datagram. At the arrival of the first IP packet at the station A HF radio, a link to the HF destination node is set up by Connection Management messages. Then a datagram containing the first IP packet is transferred from A to B, for example by using two HDL6 frames, each followed by an ACK frame in the reverse direction. This event is followed by an end-of-message transmission, indicating that the successful transfer of this first STANAG 4538 datagram is complete. After a waiting period T_w (to allow for a possible reversal of the channel), link management messages are again exchanged to arrange for the transfer of the next datagram from station A, containing the second IP packet. This procedure repeats until all IP datagrams have been successfully transferred, after which time the channel management initiates a release of the channel.

The above procedure obviously leads to a significant increase in the transfer time of the 4406 message, compared with what is achievable if the STANAG 4538 protocols would send the message as one datagram. The main reasons for this degradation of throughput are:

- A significant portion of the transfer time is spent in conjunction with the multitude of connection management messages and end-of-message transmissions.
- The frame length of the data link protocols of STANAG 4538 have discrete values, so that the last frame in a datagram will normally be padded. The corresponding degradation of throughput depends on the HDL/LDL frame used and the IP packet length.
- Short IP packets will represent a particularly poor match to HDL protocol frames, the minimum length of which is 699 bytes. The low throughput LDL protocol may be the preferable choice even on good HF channels when a long message is constituted of many short IP packets. For a channel without errors, LDL256 give a similar or better throughput value to HDL3 at IP packet sizes below 250 bytes.

Fig 5 shows an example of the potential throughput on an error free HF channel as a function of the IP packet size. HDL protocols are used to transfer one UDP/IP packet per frame. The message size used for the calculation is 15 000 byte. However, the link throughput is not very sensitive to the size of the message as long as the message comprises more than a few IP packets.

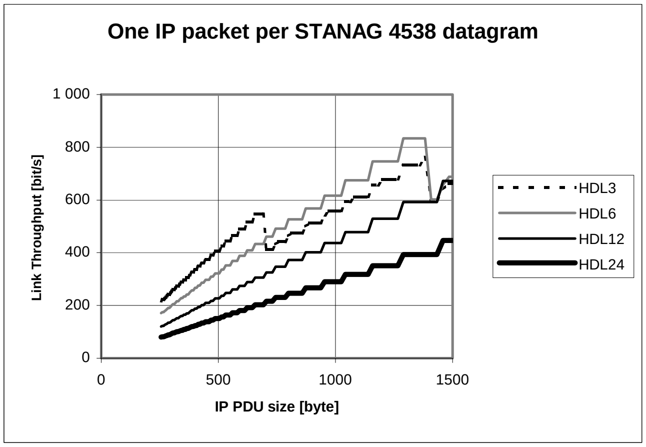

Figure 5: Throughput of HDL protocols when transferring one UDP/IP packet per STANAG 4538 datagram. No channel errors.

Figure 5 covers the most common range of IP packet sizes; the maximum IP PDU size of Ethernet being 1500 byte. It is noted that the maximum throughput (given by HDL6 and HDL12) is rather low, at least compared with the capacity that otherwise might be achieved with the STANAG 4538 HDL protocols. For example, transmitting the message as one single STANAG 4538 HDL datagram will significantly increase the throughput capability. In Figure 1, the average throughput of a 15 000 byte HDL message transfer on an ideal HF channel is in excess of 2.200 bit/s.

The above example illustrates the fact that a STANAG 4538 subnet transfer of one IP packet per STANAG 4538 datagram does *not* provide a very efficient solution on good HF channels. However, there are means to increase the throughput of IP packets. When two or more IP packets are waiting to be serviced to the same link destination, these should be combined into one datagram for transmission on the HF channel. For applications using the UDP transport service, such as the STANAG 4406 Annex E, this concatenation of packets will be particularly attractive.

In order for the STANAG 4538 to offer a more efficient service in an IP network, a method for concatenating packets should be introduced. To achieve interoperability, a protocol handling the concatenation must be standardized. It is suggested that a future version of the STANAG 4538 should address this issue.

We have measured application throughput for various file sizes between the STANAG 4406 Servers. Figure 6 shows the throughput of both STANAG 4406 Annex E (tactical) and Annex C (full OSI stack) protocols on an error free channel. Note the logarithmic scale on the vertical axis. We observe that the measured throughput of long messages using Annex E is higher than what is possible by transmitting one IP packet per STANAG 4538 datagram (ref Figure 5). Hence, the HF radio software contains a protocol for concatenation of IP packets.

Source Quenches from the transmitting radio are invoked at file sizes larger than 9000 bytes. In the tested version of the radio software IP packets are then discarded and needs to be retransmitted by the application. Even though the retransmitted PDUs are only transmitted once on the HF link, it will nevertheless cause a loss in protocol efficiency. This is visible in Figure 6 as a loss of throughput of message sizes of about 9000 bytes and above for the Annex E measurements. The time used for channel selection in the radio has not been studied, but it introduces a variability in the measurements of a few seconds.

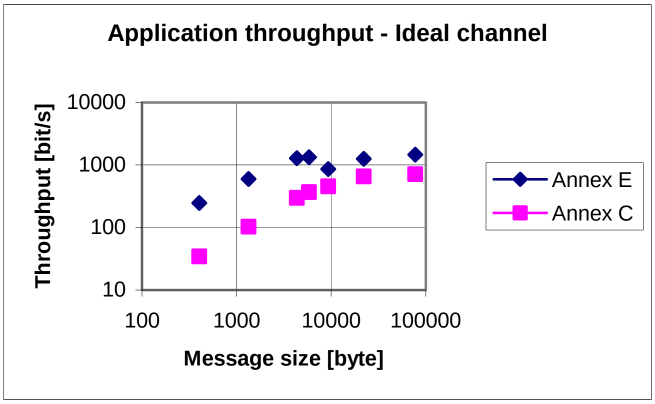

Figure 6: Measured throughput of STANAG 4406 across a STANAG 4538 HF link. Ideal channel.

For the 9000 byte file the maximum unidirectional link throughput measured when transmitting IP is in the order of 1550 bps. In this figure the time used for application ACK and link establishment/release has been disregarded.

The relative advantage of using the tactical profile (Annex-E) compared to the full OSI stack (Annex-C) is largest for the smallest file sizes where the throughput increases with a factor of seven.

The following radio software implementation choices were found to influence the measured throughput:

- the link protocol and the concatenation of IP packets, as described earlier
- the radio buffer size and the rules for composing the first packet
- allowing for traffic reversal (advantageous for TCP/IP) between consecutive link datagrams

In addition, a number of parameters of the Annex E protocol such as the offered packet rate, packet length and the source quench reactions will influence the overall performance.

CONCLUSIONS

The Military Message Handling System defined in NATO STANAG 4406 is intended to run over different bearers, one of them being HF. Our work has shown that it is very important to test and understand how the whole protocol stack from application to bearer work together, in order to obtain an efficient C2IS. We have discovered several optimization issues at different levels of the protocol stack, and that throughput numbers are very dependant on implementation choices.

To make HF an integrated part of the Tactical Internet, an IP multicast service should be provided as part of STANAG 4538. Also, for improved throughput of IP packet transfer, further standardization of STANAG 4538 data link protocols is required to ensure interoperability.

REFERENCES

1. NATO Standardization Agreement (STANAG) 4538, Technical standards for an automatic radio control system (ARCS) for HF communication links, Ed. 1

2. NATO Standardization Agreement (STANAG) 5066, Profile for high frequency (HF) radio data communications, Version 1.2

3. NATO Standardization Agreement (STANAG) 4406, Military Message Handling System (MMHS), Ed. 1, 1999

4. Chamberlain M. W., Furman W. N., Palum L.F., Robertson G. R., 2000, IEE Conf Publication No 474, 145-149

5. Mil-Std-188-141B, Interoperability and performance standards for medium and high frequency radio systems,

6. Allied Communication Publication (ACP) 127 (G), Communication Instructions Tape Relay Procedures

7. Allied Communication Publication (ACP) 142 v.1.0, P_MUL: An Application for Multicast Messaging under EMCON Restriction, 2000

Acknowledgements

We would like to thank Eric Koski and Eric Peach at Harris Corp., Rochester, N.Y. for very efficient help and support during this work. Thanks also to Asgeir Langen at Thales Communications, Trondheim, Norway.

B APPENDIX

MILITARY MESSAGING IN IP NETWORKS USING HF LINKS

Military Messaging in IP Networks Using HF Links

Vivianne Jodalen, Anders Eggen, Bjørn Solberg, and Ove Grønnerud,
Norwegian Defense Research Establishment

ABSTRACT

In the migration toward network-centric warfare, the NATO STANAG 4406 for Military Message Handling Systems (MMHS) may be used for direct information exchange between high-data-rate strategic users and low-data-rate tactical users by utilizing its new tactical protocol profile. In this article the protocol profiles are tested across a "worst case" tactical HF link providing IP services. There are considerable throughput gains available using the tactical profile. Among the various automated HF technologies tested, the new HDL+ data link protocol, suggested for standardization within NATO, shows the best throughput capabilities for short to medium-size messages on typical HF channels. 3G HF is the most robust technology at low signal-to-noise ratios. The 2G HF throughput performance suffers from inefficient linking procedures. There are optimization issues at different levels of the protocol stack, and implementation choices have great impact on overall performance.

INTRODUCTION

The network-centric warfare (NCW) concept focuses on information and makes information exchange even more important than in the command and control systems of today. The concept of operations is based on the assumption that information superiority will lead to higher speed of operations and increased combat power. One of the major challenges will be to find ways to distribute the relevant information to all involved parties, in order to achieve shared awareness and make decisions based on a common operational picture. The involved forces may be out in the field or operating within a strategic environment. It is clear that increased interoperability between strategic and tactical systems will be necessary, including distribution of information over different types of communication systems with variable quality and data rate.

Many nations have a migration plan toward NCW, and some existing systems will continue to be used for a long time because of the investments in these systems. One such system is the NATO formal Military Message Handling Systems (MMHS) based on Standardization Agreement (STANAG) 4406 [1]. The reason for this assumption is that most NATO nations (including the NATO organization) recently have procured, or are in the process of procuring, systems in accordance with this standard. S4406 includes both strategic and tactical protocol profiles, which may be used for exchanging information between high-data-rate strategic and low-data-rate tactical domains.

This article will focus on how the MMHS may be used over a low-data-rate high-frequency (HF) system, as we consider this to be one of the worst-case tactical links.

IP will be the integrating networking technology in future military communications networks. We therefore discuss the use of IP as an integrator between MMHS and HF, since many nations are planning to use IP as a platform for their communication systems in both the strategic and tactical domains. A demonstrator is used to show the concept, and results from throughput measurements are presented.

TACTICAL RADIO COMMUNICATIONS

Tactical communications is used by highly mobile units not able to utilize a fixed communications infrastructure. Typical tactical units are naval vessels, aircrafts, land mobiles, and special forces carrying manpack radios. Typical characteristics of long-range tactical radio communications in general are:

- Only low to moderate data rate is supported (< 10 kb/s)
- Variable data rate depending on time, location, and other users of the radio spectrum
- Unreliable connections; high bit error rates, frequent link terminations, unreachable nodes, equipment failure
- Half-duplex or simplex channels, giving large turnaround times
- Different types of radio equipment

Operationally, EMCON (radio silence) conditions are often required for tactical users of the radio spectrum.

The above characteristics apply to HF communications in particular, since HF propagates via reflecting layers of the ionosphere that support a very limited data rate. HF radio systems normally operate in half-duplex mode. Under very favorable conditions, a maximum of 9.6 kb/s user data rate can be achieved in a 3 kHz channel. The data rate is normally much lower due to absorption of the signal, manmade noise, and interference. Also, rapid time fading of the signal and excessive multipath impose a reduced data rate.

MILITARY MESSAGE HANDLING SYSTEMS EXTENDED TO TACTICAL USERS

A formal military message is different from an interpersonal message in that it is a message sent on behalf of an organization, and it establishes a legal commitment on the sending and receiving organization under military law. Examples of formal messages are military orders.

Formal military messages are handled by MMHSs. An MMHS is responsible for the delivery, formal audit, archiving, numbering, release, emission, security, and distribution of received formal messages. In NATO, the formal messaging service is seen as the vehicle for secure mission-critical operational, military applications (email systems are not). S4406 Edition 1 is the only agreed standard to achieve interoperability between the formal messaging systems of NATO nations. Systems compatible with the S4406 standard have been and are being implemented widely by the NATO nations and the NATO organization. With the inclusion of a tactical protocol profile in Annex E of S4406, a common baseline protocol solution exists that opens up use of the MMHS in both the strategic (fixed) and tactical (mobile) environments. One messaging system may therefore be used to communicate with all national forces, the NATO organization, and the NATO allies.

In addition to military messaging, an MMHS may also be used as an infrastructure for interconnection of other applications by use of a standardized application programming interface (API). In this perspective, the MMHS may be viewed as a type of middleware system, which may tie the applications together and be used over communication systems with different qualities and data rates. This may be an important feature in the migration process toward NCW.

An MMHS message transfer agent (MTA) is a switch in the message transfer system. It is a store-and-forward application, and may be used as a gateway between the strategic and a tactical messaging system. The MTA may have a dual protocol stack implementing both the strategic connection-oriented protocol profile (S4406 Annex C) and the tactical connectionless protocol profile (S4406 Annex E). This MTA may therefore route messages between the strategic and tactical MMHS systems (Fig. 1). This concept was first demonstrated at the Joint Warrior Interoperability Demonstration (JWID-02) [2] and will be fielded in Norway in order to integrate the strategic and tactical MMHS of the Norwegian Army and Navy.

The original connection-oriented protocol stack defined in S4406 Annex C (and ACP 123 [3]) was developed for strategic high-data-rate networks and is not suitable for channels with low data rates. The protocol solution defined in Annex E of the S4406 has therefore been developed for *tactical* communications.

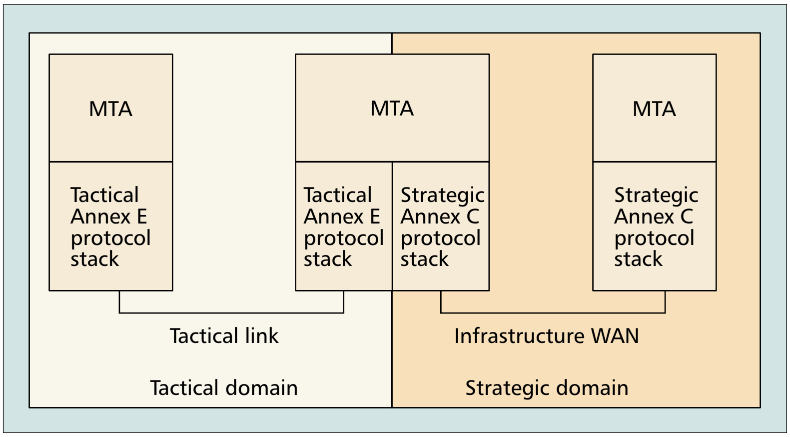

Figure 1. *Seamless interconnection of MMHS between the strategic and tactical domains.*

To take account of the characteristics of a tactical radio link, the tactical protocol profile of S4406 Annex E has adopted the following:

- A connectionless protocol stack, which gives less overhead and reduces the effect of large turnaround times of the link
- A choice of full-duplex, half-duplex, or simplex (broadcast) operation
- Compression to reduce the amount of data transmitted
- Usable for both unicast and multicast, the latter providing efficient use of radio resources
- Procedures for handling EMCON recipients

These features of Annex E increase the messaging throughput substantially for tactical communication channels with low data rates compared to the connection-oriented Annex C protocols.

Figure 2 shows the layered architecture of the S4406 Annex E protocol profile. The profile is divided into an application layer and a transport layer on top of the potential bearer systems. The application layer is further divided into more specific sublayers.

The messaging sublayer is kept the same in Annexes E and C in order to reuse the messaging applications. The tactical adaptation sublayer does the required protocol adaptation in order to keep a common service interface (TA-SAP) for the different protocol stacks. In addition, this sublayer performs compression and decompression of the whole message (both envelope and content).

Since the connection-oriented protocol stack is removed, the transfer reliability it provides is also removed. However, this is compensated for by the introduction of the P-Mul sublayer. The P-Mul protocol is defined by the military standard ACP 142 [4]. This sublayer has functionality for both multicasting and unicasting of messages. It splits the message into smaller protocol data units (PDUs), attaches a checksum, numbers the PDUs, and handles retransmissions based on a selective repeat procedure.

Because P-Mul is responsible for reliable message delivery, the transport layer of Annex E

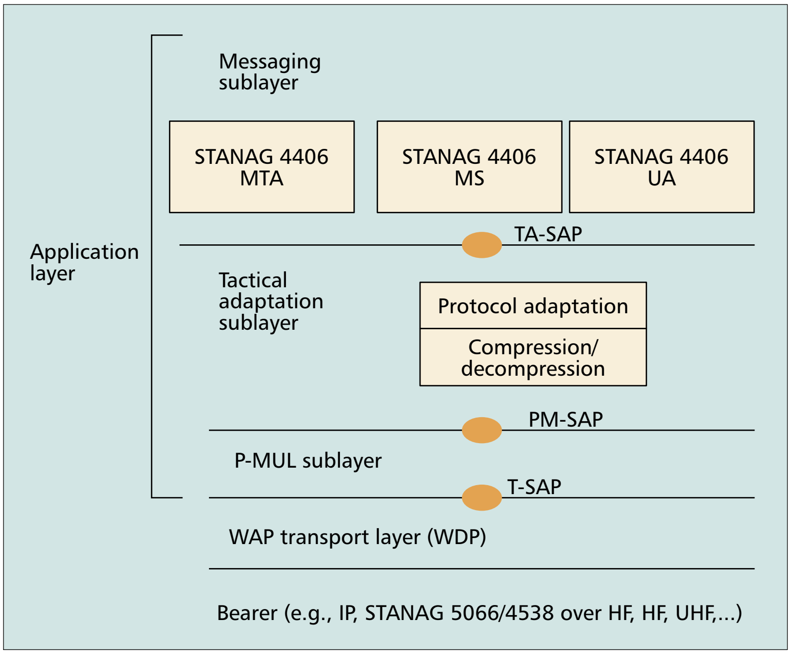

Figure 2. *The protocol structure of STANAG 4406 Annex E.*

uses a connectionless wireless application protocol (WAP) called the Wireless Datagram Protocol (WDP). This protocol is more flexible than the UDP protocol in that it does not mandate the use of IP. If IP is used, however, the WDP protocol becomes UDP. In our test where the HF radio provides an IP service, Annex E uses the UDP protocol.

There are several reasons for not using the standard TCP protocol in the Annex E stack, the most important of which are:

- TCP performs poorly on many tactical channels, mainly due to an inefficient retransmission mechanism and its underlying presumption that all lost packets are caused by a congestion problem.
- Because TCP is connection-oriented, it will not support multicasting or handle traffic to recipients in radio silence.

2G AND 3G HF NATO STANDARDS

Traditionally, HF communications required a highly skilled operator to establish and maintain an HF link. Over the last two decades automation of processes such as channel selection (ACS), link establishment (ALE), link maintenance (ALM), and data rate adaptation has made the skilled operator superfluous. NATO has developed a family of standards at the physical and data link layers within the "HF-House" concept. Many of the standards (STANAGs) have a U.S. MIL-STD counterpart, and some of the MIL-STDs have been adopted directly by NATO. The HF-House covers what is called second-generation (2G) HF and third-generation (3G) HF technology, both of which contain descriptions on automated procedures at the link level, appropriate waveforms to be used at the physical level, and how the HF subnetwork can interface a data network. 2G technology has existed for a longer period of time than 3G, but is not considered to be obsolete because of 3G. It is predicted that 2G and 3G will coexist in the years to come and have different usages. We describe some main differences between 2G and 3G in Table 1.

A common operational configuration of a 2G HF system is based on the following set of HF standards: MIL-STD 188-141A [5] for link setup, STANAG 5066 [6] as a data link protocol including automatic repeat request (ARQ) and automatic data rate adaptation, and STANAG 4539 [7] for waveforms. In addition, according to STANAG 5066, if IP is going to be transmitted, IP packets delivered to the HF subnet (S5066) must be "wrapped" into standardized primitives. For this purpose a dedicated IP client to the HF subnetwork must be used.

For 3G HF, STANAG 4538 [8] includes link setup, a data link protocol including ARQ, data rate adaptation, and burst waveforms. The 3G

2G automatic HF	3G automatic HF
Modular, different functionalities may be located at different pieces of hardware	Integrated, all functionalities located in the radio
Asynchronous calling, no GPS time reference, gives longer call times	Synchronous calling, uses GPS time reference, gives short call times for members of the net
Linking using 8-FSK, not particularly robust at low SNRs	Linking using 8-PSK and Walsh functions, very robust at low SNRs
Data rate adaptation based on an explicit change of waveform, slower than for 3G	Data rate adaptation based on adapting the code rate (code combining), fast adaptation
Can utilize high-data-rate waveforms (up to 12,800 b/s) defined in STANAG 4539	Is limited to a maximum data rate of 4800 b/s defined by the burst waveforms
Offers a point-to-point service and a broadcast service for both packet- and circuit-switched data	Offers a point-to-point service for packet- and circuit-switched data and a point-to-multipoint service for circuit-switched data only
Allows a more flexible frame size of forward transmissions, throughput efficient	Finite number of forward transmission sizes, less throughput efficient

Table 1. *Characteristics of 2G vs. 3G automatic radio systems at HF.*

implementation used in our tests includes a direct IP interface to the radio, making the radio act as an IP router.

The current version of STANAG 4538, Edition 1, includes waveforms with a maximum gross data rate of 4800 b/s. In a future edition of the STANAG, a new data link protocol providing higher throughput and lower latency has been proposed and will be incorporated. The protocol has been designed to support efficient exchange of IP-based data traffic. Harris Corporation has developed and implemented this data link protocol, called HDL+ [9]. The basic idea of the protocol is to combine the high-data-rate waveforms of STANAG 4539 with some code combining technique to give an adaptive data link protocol capable of error-free delivery up to 10,000 b/s in a 3 kHz channel. HDL+ gives significantly higher throughput than standardized 3G technology for high signal-to-noise ratios (SNRs). For low SNRs the HDL+ protocol resorts to standardized 3G protocols. The protocol is still under development, and future refinements such as bidirectional data transfer will further improve its capability to support TCP/IP-based applications.

Because of the special characteristics of HF links, many standard applications work poorly over them. For this reason, the HF community has defined application stacks tailored for HF communications, which therefore offer improved performance. Examples of such applications are the HMTP and CFTP protocols defined in STANAG 5066, which are variants of the Simple Mail Transfer Protocol (SMTP) email application. These applications are effectively interfaced with the standardized data link protocols at HF without any intervening transport and networking protocol such as TCP/IP or UDP/IP.

However, in an NCW scenario, and particularly for tactical communication users, applications unique to each bearer service are not desirable. It is operationally more attractive to use one application able to select the most appropriate bearer service at any time. For this purpose, extending IP-based networking to tactical communications is very interesting.

IP OVER HF

The arrival of fully automated and adaptive HF systems may enable an HF link to constitute an integral part of a military IP network. Due to the extraordinary radio coverage of HF, such a solution could offer IP services to users positioned well beyond line of sight, which is considered the range limit of many communications systems at higher frequencies.

IP over HF is an interesting alternative, for instance, for:

- Future shore-ship/ship-ship communications
- Communications to special forces in hostile territory
- Last-ditch communications when the normal communications grid has broken down

Even with the improvements offered by HF modem technology, the throughput of the typical HF link will be very low and the latency very high compared to most other links used in an IP network. In most cases the HF link will inevitably represent a bottleneck in the IP network, with a great impact on the quality of service offered to the user.

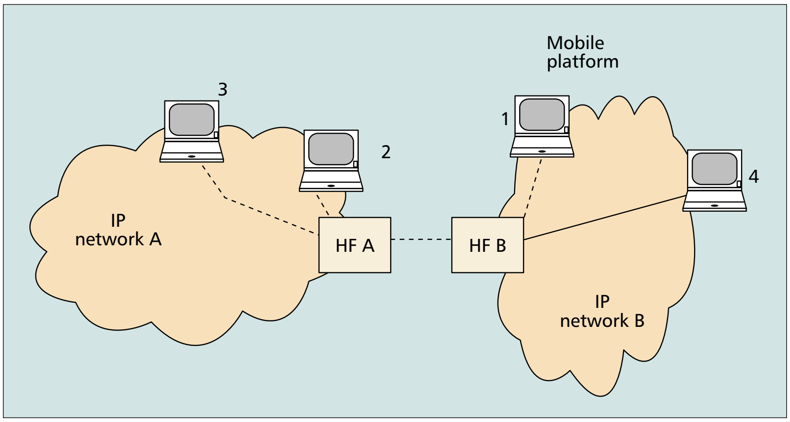

Figure 3. *A model of IP networks connected by HF.*

Consider the simple model of the network outlined in Fig. 3, in which an HF link is used to connect IP networks A and B. Using 2G or 3G HF protocols, IP connectivity may be offered between data terminals (2, 3) in the main network and terminals (1, 4) residing on the mobile platform (e.g., a ship). In order to take advantage of this IP service, the protocols above the network layer must be able to tolerate the high latency imposed by the HF link protocols. In order to achieve satisfactory performance in an IP networking situation, parameter tweaking may be necessary for the HF link protocols as well as the transport protocols.

The nodes HF A and HF B in Fig. 3 each comprise the HF radio/modem functionality, the HF link protocols, an optional link crypto functionality, and finally, an IP routing functionality. The 3G HF system presently available has all these functionalities embedded. Consequently, the 3G HF node is simply composed of a dedicated HF radio, which then also acts a IP networking component. A state-of-the-art 2G node, however, has its networking functionality and its HF protocols running on separate PCs. In this case the HF radio merely offers a physical layer service transferring either a digital bitstream or an analog signal from one node to the other.

In Fig. 3, terminals 1–4 are data terminals, two of which host a STANAG 4406 MTA for provision of seamless MMHS service to the mobile platform.

THROUGHPUT MEASUREMENTS

The measurements reported in this article aim at exploring the efficiency of the message transfer protocol stack of the MMHS, the HF link protocols, and the interactions between them.

Compressed messages were transferred between terminals 2 and 1 in Fig. 3, and the transfer times were recorded. The HF protocols could select channels from a pool of 10 frequencies. The application level throughput was calculated as the compressed message size divided by the delivery time. Since the message is delivered before all the protocol layers have been released, the real occupancy of the HF channel is some-

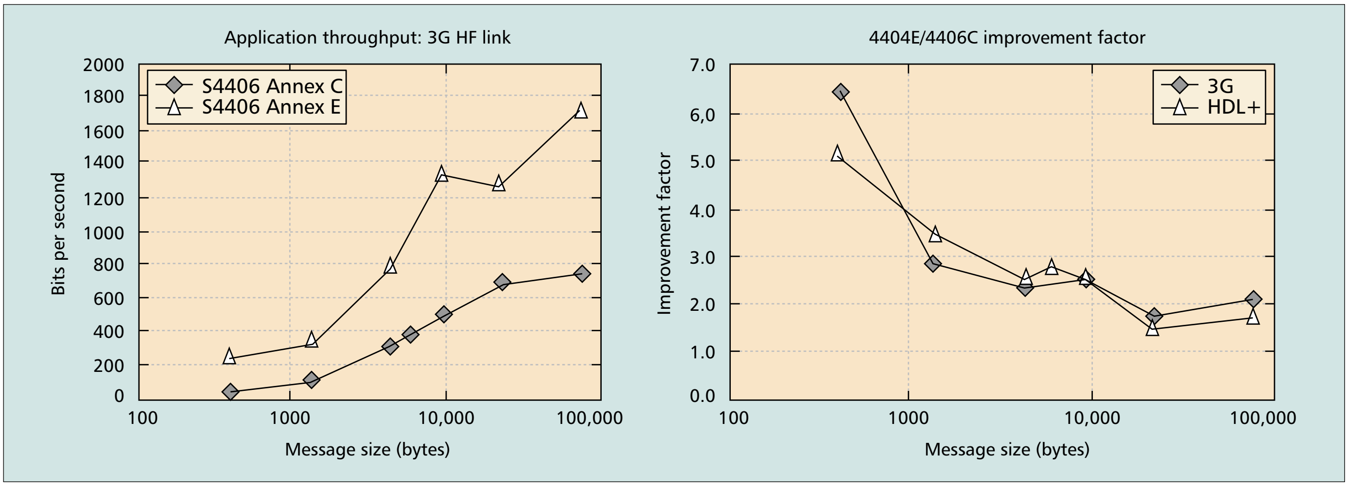

Figure 4. *Measured application throughput (left) and relative performance improvement (right) on a 3G link on a perfect HF channel for the two different protocol stacks defined in STANAG 4406.*

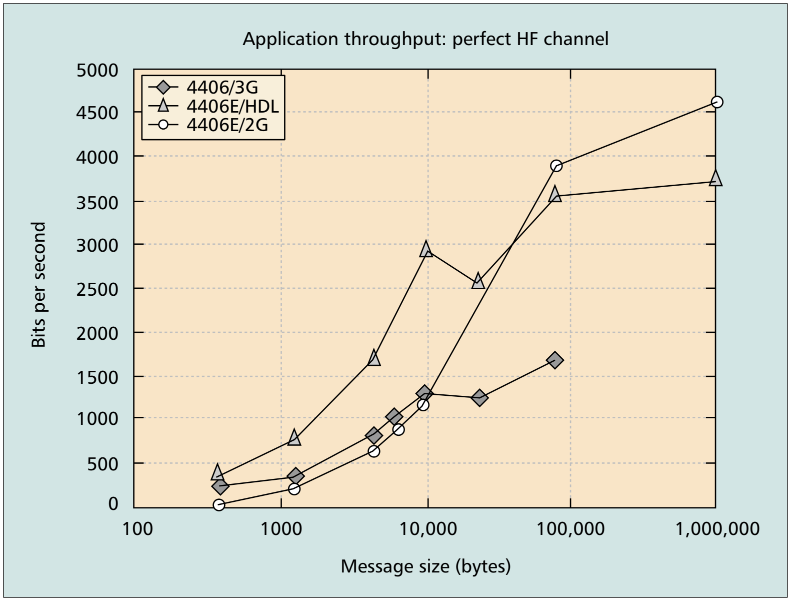

Figure 5. *Message throughput using STANAG 4406 Annex E protocols on an "ideal" HF channel.*

what longer than the transfer time, making our throughput calculations slightly optimistic. This will be particularly noticeable with short messages transferred by the S4406 Annex C protocols.

The transfer times measured are affected not only by the protocols in use and channel conditions, but also by configuration parameters and implementation choices made by the equipment vendors. For example, the HF standards define only a number of different waveforms, but the choice of when to use the various waveforms is left to each implementation. Also, the results depend on the parameters of the MTA, such as the IP packet rates and packet size. Consequently, the throughput measured is only indicative of what can be obtained, and does not serve as a definite upper limit.

The messaging application used during the measurements was the XOmail Thales implementation of S4406, including both the tactical (Annex E) and strategic (Annex C) protocol profiles. For the 2G tests, the IP packets were sent to the NC3A IP client [10], which encapsulated the IP packets within S5066 service primitives and forwarded them to the Harris S5066 protocol stack. The HF radio used was the Harris RF-5800H-MP, which includes embedded implementations of 3G, HDL+, and 2G link setup. The tests were performed over a white Gaussian noise channel, allowing the SNR to be controlled. No fading or multipath conditions were applied.

Figure 4 illustrates how the throughput on a 3G HF connection transferring IP packets is affected by the S4406 protocols. The HF channel is "perfect" in the sense that it supports the highest modem data rates without introducing bit errors. The increased performance offered by the Annex E protocols is evident. The throughput improvement factor using the Annex E protocols compared to the Annex C protocols when operating on 3G and HDL+ systems is also shown in Fig. 4. The improvement is particularly significant for short messages. The improvement factor increases as the HF channel deteriorates, so on a typical HF channel the improvement factor will be higher than the levels shown in Fig. 4.

Our next observation focuses on the different HF link protocols (2G, 3G, HDL+) as the carrier of the S4406 Annex E message traffic. Figure 5 shows how the message throughput varies with the message size when the HF link protocols operate on a channel supporting error-free transfer at the highest modem rate. For a large message size the 3G protocol offers less throughput than the 2G and HDL+ protocols. The HDL+ protocol outperforms the 2G for low to medium-sized messages because of its superior link establishment time. The reason for the dip in 3G/HDL+ performance curves above 10 kbytes is not related to the 3G/HDL + protocol, but to an undesired interaction between the Annex E implementation and the radio's IP interface. The basic cause of this problem is the lack of a good flow control method in the Annex E protocol stack, which is described in detail in the next section. Tweaking parameters in the P-Mul protocol can enhance the throughput performance for large messages. The 2G measurements do not suffer from a similar penalty in throughput, because the implementation of the IP client can accept larger files without need of flow control.

Figure 6 presents the measured throughput for a 9.3 kbyte message transfer on an additive white Gaussian noise (AWGN) channel. Using the HDL+ protocol will provide the best performance at positive SNRs. At negative SNRs the 3G and HDL+ protocols provide similar throughput. The 2G protocol is less robust than the 3G protocol. At positive SNRs the 2G and 3G protocols give a more or less similar performance for this file size, in spite of the much higher link establishment time of the 2G protocol.

Some other issues related to use of the S4406 Annex E in IP networks over tactical links will be addressed in the next section.

FLOW CONTROL ASPECTS

The HF link will constitute an extremely narrow and rather unpredictable "pipe" unable to serve traffic at the normal rates of IP networks. Normally, IP packets will arrive at a higher rate at the HF transmit node than the node is able to support; hence, packets will accumulate in buffers at the HF node. With respect to the throughput of the HF link, this is in fact desirable, because the HF protocol efficiency improves when an HF frame transmitted over the air is large and comprises an assembly of several smaller IP packets.

However, since neither P-Mul nor UDP has mechanisms for flow control or network congestion control, buffers in the HF transmit node will tend to overflow and packets will be discarded for long messages. Some other means of adjusting the packet rate from Annex E is needed in order to achieve balance between maximum throughput on the HF link and buffer overflow.

Consider a message transfer from MTA 2 to MTA 1 in Fig. 3. In order to take full advantage of the capabilities of the HF link, MTA 2 needs to offer a packet rate exceeding the maximum throughput capabilities of the HF link. However, in this case, when long messages are transferred, the buffers of radio HF A (or of the IP client of the HF subnetwork) will tend to overflow. When this occurs, HF A will discard the subsequent packets at a high rate. Although the discarded packets will be retransmitted by P-Mul, this effect may severely deteriorate the overall performance of the Annex E protocol stack.

The present implementations of the Annex E protocol and the HF node work around this problem by making use of the IP control message protocol (ICMP). When the buffer of HF A overflows, a Source Quench message is generated and sent to the originating end terminal. This message is used to instantaneously reduce the packet flow from P-Mul, thereby minimizing the influence of the buffer overflow problem.

The buffer size of the HF radio in our 3G and HDL+ setups was about 10 kbytes. For larger file sizes, the HF radio generated a Source Quench message, which was used to reduce the rate of packets from the MTA. The buffer size of the IP client of the HF subnetwork was much higher than that of the 3G radio, and no packets were discarded in the 2G measurements. The 3G/HDL+ results of the previous section include the effects of packet discarding and source quenching.

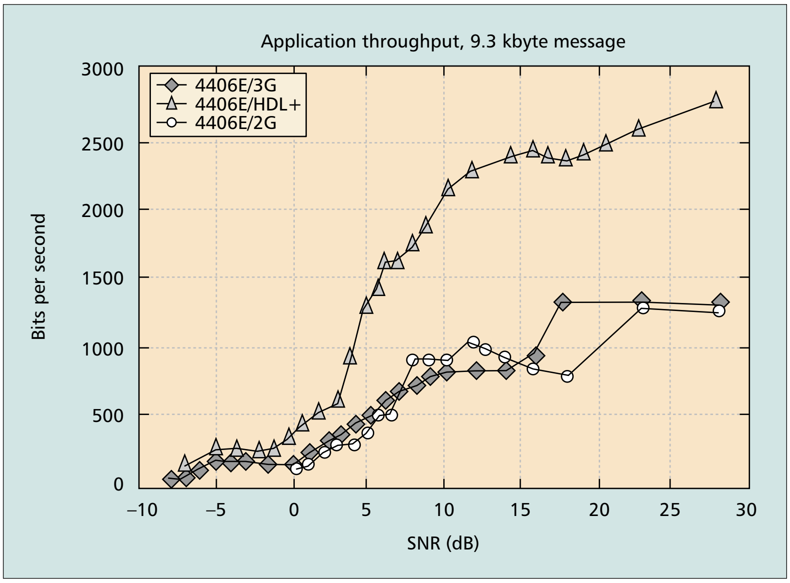

Figure 6. *The message throughput as a function of the SNR on an AWGN HF channel. The message size is 9.3 kbytes.*

Although not perfect, by using the Source Quench mechanism for flow control a reasonably high throughput capability will also be achieved when transferring long messages using the Annex E protocols. The impact on performance of this type of flow control is evident in Fig. 5, where the throughput curve for the 3G/HDL+ systems drops for message length exceeding the buffer size of 10 kbytes. This deterioration in throughput could be reduced or even avoided by letting the HF radio issue Source Quench messages when the buffer approaches overflow rather than waiting until an overflow situation has already occurred.

There are, however, unresolved issues regarding the use of the Source Quench mechanism in combination with IP security devices in military networks. These devices will normally not allow the transfer of a Source Quench message from a "black" network element (the HF radio) to terminals in the secure part of the network, leaving this mechanism useless in these types of situations. Therefore, in the longer term, the functionality of the P-Mul protocol should be extended to include its own mechanism for flow/congesting control allowing efficient transfer of longer messages over tactical IP networks in all kinds of situations.

MULTICAST

In order to make a tactical radio network such as HF an integrated part of an overall IP network, the services available in the overall network should, to the largest extent possible, also be available in the HF subnetwork. Multicasting may be a bandwidth-efficient way of transferring messages intended for several different destinations provided that the underlying network also offers a multicast data transfer service.

Annex E of the MMHS supports multicasting, but can also be run in unicast mode. In both

Our work has also shown the importance of testing complete systems together, ranging from application to the physical link. There are optimization issues at different levels of the protocol stack, and we have seen that implementation choices have great impact on the overall performance of the system.

cases an efficient acknowledgment and retransmission protocol is applied at application level.

The data link protocol of 2G HF systems defines a non-ARQ broadcasting protocol, but 3G HF does not presently define a multicast or broadcast packet data service. This prevents the use of the multicast features of Annex E together with 3G HF. A future multicast packet service is highly desirable in 3G HF technology, and it is currently being worked on in NATO.

CONCLUSIONS

The military message handling system (MMHS) based on STANAG 4406 offers seamless connectivity between strategic and tactical users of the system. The tactical protocol profile (Annex E) of this standard has been shown to give considerably larger throughput on a worst case tactical link than the companion strategic protocol profile (Annex C). The improvement is particularly significant for short messages. For 1 kbyte messages, using the Annex E profile on a 3G HF link will improve the message throughput by a factor of at least four compared to the S4406 strategic protocol profile.

The MMHS is able to utilize different networking technologies. Since IP will be the integrating networking technology in future military communications networks, our test setup included two HF systems, 2G and 3G automated HF, offering IP services.

For the transfer of large messages on an HF link as part of an IP network, Annex E performance is vulnerable to its lack of flow control mechanisms. Other means of flow control is necessary. The flow control mechanism used in the tests was based on the use of the ICMP Source Quench message. However, optimization of the quenching parameters is necessary if throughput degradation is to be minimized.

Conclusions regarding the throughput of military messages using UDP/IP across the various HF systems are (over a white Gaussian noise channel):

- 2G automatic link establishment causes significant delay and reduces the throughput of the 2G system tested, in particular for short and medium messages.
- On good channels and with short to medium message sizes, HDL+ achieves throughputs significantly greater than those achieved using 2G. For higher message sizes the measured performance of HDL+ and 2G was more or less similar. However, it should be noted that the measured throughput values on the HDL+ system were limited by imperfect flow control between the message transfer agent and the HF radio, preventing the HDL+ protocol from operating with maximum efficiency for message sizes above 10 kbytes.
- 3G HF is more robust than 2G at negative SNRs. This is true whether or not HDL+ is enabled, since HDL+ is not used at the lowest SNRs.
- HDL+ significantly improves throughputs on channels with positive SNRs compared to the present 3G standard.

Our work has also shown the importance of testing complete systems together, ranging from application to physical link. There are optimization issues at different levels of the protocol stack, and we have seen that implementation choices have great impact on the overall performance of the system.

ACKNOWLEDGMENT

Thanks to Harris Corporation and Thales Norway for technical support of this work.

REFERENCES

[1] NATO STANAG 4406, "Military Message Handling System (MMHS)," ed. 1, 1999.

[2] A. Eggen *et al.*, "The Joint NO and UK Demonstration of Integrated MMHS, PKI and Directory Systems at JWID 2002," FFI/RAPPORT-2002/04655, 2002.

[3] Allied Commun. Pub. (ACP) 123, "Common Messaging Strategy and Procedures, Combined Communications Electronic Board (CCEB)."

[4] ACP 142 v. 1.0, "P-Mul: An Application for Multicast Messaging under EMCON Restriction," 2000.

[5] US MIL-STD-188-141A, "Interoperability and Performance Standards for Medium and High Frequency Radio Equipment," App. A.

[6] NATO STANAG 5066, "Profile for High Frequency (HF) Radio Data Communications," v. 1.2.

[7] NATO STANAG 4539, "Technical Standards for Non-Hopping HF Communications Waveforms," ed. 1.

[8] NATO STANAG 4538, "Technical Standards for an Automatic Radio Control System (ARCS) for HF Communications Links," ed. 1.

[9] M. W. Chamberlain and W. N. Furman, "HF Data Link Protocol Enhancements based on STANAG 4538 and STANAG 4539, Providing Greater than 10 kb/s Throughput over 3 kHz channels," *IEE Conf. Pub. No 493*, Bath, U.K., 2003, pp. 64–68.

[10] J. W. Smaal, "STANAG 5066 IP Subnet Client, SISmcast," Application Note, NC3A, http://elayne.nc3a.nato.int

BIOGRAPHIES

VIVIANNE JODALEN (vivianne.jodalen@ffi.no) is a senior scientist at the Norwegian Defense Research Establishment (FFI). She received an M.Sc. degree from the Department of Electrical Engineering, Norwegian Institute of Technology, Trondheim, Norway, in 1987. She has been employed at FFI since 1988, and her working experience is within radio wave propagation, HF systems, and communication protocols. In 1996 she received a Ph.D. from the Institute of Physics, University of Oslo. She has participated in technical standardization of HF systems within NATO.

ANDERS EGGEN (anders.eggen@ffi.no) received his M.Sc. degree in computer science from the Department of Informatics, University of Oslo in 1991. Since 1992 he has worked for the Norwegian Defense Research Establishment (FFI), where he is currently a principal scientist. At FFI he has worked on many aspects of network, communication and application protocol evaluation and design. He has contributed significantly to standardizations activities in both NATO and IETF, and has been editor and co-editor to several IETF and NATO standards (including STANAG 4406 Annex E, discussed in this article).

BJØRN SOLBERG (bjorn.solberg@ffi.no) received his M.Sc. degree in electronic engineering from the Norwegian Institute of Technology, Trondheim in 1968. He works as an independent consultant at Telesystemer AS, Oslo, and has 20 years of experience with specifications and system design of tactical radio communications systems in various frequency bands. His current main interests include performance evaluation and protocol design for wireless data communications.

OVE K. GRØNNERUD (ove-k.gronnerud@ffi.no) is a principal engineer at the Norwegian Defense Research Establishment (FFI). He was educated at Oslo University College in 1967 within the radio electronics field. Since 1968 he has been employed at FFI. In his first two decades there he did digital hardware design, mainly in the communication field. The first task was as a member of a group designing a 16-bit digital computer. In the last decade he has been responsible for the design of test systems for radio communication systems ranging from HF to SHF.

C APPENDIX

ON-AIR TESTING AND COMPARISON OF 2G AND 3G HF

ON-AIR TESTING AND COMPARISON OF 2G AND 3G HF

Vivianne Jodalen, Bjørn Solberg and Ove Grønnerud

Norwegian Defence Research Establishment (FFI)
P.O Box 25
N-2027 Kjeller
Norway
vjo@ffi.no, bso@ffi.no, okg@ffi.no

SUMMARY

The HF STANAG's 5066 (2G) and 4538 (3G) can provide a transparent IP service across an HF subnet. We have explored the possibilities and performance of a NATO standardized application, the Military Message Handling System defined in STANAG 4406, when run over an HF link supporting IP. In addition to a 2G and a 3G HF system, we have also tested a new data link protocol, HDL+, over-the-air on an NVIS path in Norway. Measurements of throughput have shown that 2G HF suffers from long linking times deteriorating the overall throughput. This is particularly noticeable for small file sizes. HDL+ is superior in performance at positive SNR's. 3G gives generally less throughput than the other two at positive SNR's and file sizes larger than 10 kbyte, but is more robust at negative SNR's. Implementation choices such as the Automatic Channel Selection algorithm and data rate adaptation algorithm may have a great impact on the measured performance.

1 INTRODUCTION

Interoperability between communications equipment used by military forces from different countries is very important in todays battlefields. During the last ten years NATO has produced a number of standards (STANAG) for military information systems, ranging from applications to bearer services such as HF. The NATO "HF House" provides a family of standards for HF communications covering radio and modem functionality, data link functionality, link establishment and electronic protection measures. A subnetwork service interface is also defined that enables applications to connect to, and obtain services from the HF subnetwork. The standards represent fully automated and adaptive HF systems, and this enables HF to become an integral part of a military IP network. Due to the extraordinary radio coverage of HF, IP services can be offered to users positioned well beyond line-of-sight. Despite improved data rates offered by new modem technology, HF will nevertheless represent a potential bottleneck in an IP network.

This work aims at exploring the performance of a specific military application utilizing UDP/IP over HF. The specific application is the Military Message Handling System (MMHS) standardized in STANAG 4406 [1]. The specific implementation tested is XOmail from Thales. The application is tested over two different HF systems: 2G HF represented by Mil-Std 188 141A [2], STANAG 5066 [3] and STANAG 4539 [4], and 3G HF represented by STANAG 4538 [5]. All HF implementations are from Harris Corp. In addition, Harris Corp has implemented and proposed a new data link protocol for standardization, HDL+, giving higher throughput and lower latency. This protocol has also been tested. Previous work in this field has been published in [6].

The first sections of this paper describe some characteristics of the involved standards that are of importance to understand the measurements. Some implementation choices made by the vendors are also described.

2 2G HF

A 2G HF system consist of independent pieces of hardware and software that together make a fully automated radio system.

Automatic link establishment (ALE) is obtained by using Mil-Std 188-141A, in our setup implemented in software in the RF-5800H Harris radio. In 2G ALE, radios scan asynchronously, which means that the call signaling must be repeated until the receiving radio visits the actual channel where the call takes place. This gives longer link setup times than for 3G HF described in the next section. The ALE waveform uses 8-FSK modulation, and together with the coding and symbol rate chosen, the linking is not particularly robust at low signal-to-noise ratios.

When a link is established on a particular channel, data is transferred by the data link protocol defined in STANAG 5066 and appropriate waveforms defined in STANAG 4539. S5066 defines a subnetwork service interface that includes an IP service access point. IP datagrams must be included in service primitives before delivery to the data link protocol. The service primitives are handled by a separate software package, in our case software delivered from NC3A [7].

The data link protocol in S5066 provides efficient and reliable data delivery on a point-to-point link using Automatic Repeat Request (ARQ). The ARQ scheme provides feedback to the transmitter on the success of the transmissions and this information is used for adapting the data rate to the channel conditions. The data rate is adapted by “self-identifying” waveforms in S4539, informing the receiving modem on the actual data rate and interleaver setting of the current waveform. The data link protocol can also be run in broadcast mode where no feedback is provided from the receivers. This does not give a reliable delivery service and eliminates the mechanisms for adapting the data rate.

S4539 specifies a set of serial tone waveforms, all using PSK or QPSK modulation at a symbol rate of 2400 symbol/s. The waveforms provide data rates ranging from 75 bits/s to 9600 bits/s using different combinations of code rate, constellation and frame pattern. Used with an ARQ-scheme as in S5066, the throughput will be less than the unidirectional data rates mentioned here.

3 3G HF

3G HF is specified in STANAG 4538. Link setup, link maintenance, data link protocol and waveforms are all defined in the same standard, and there is a close relationship between the data link protocol and the waveforms. In the only commercially available implementation of S4538 today, from Harris Corp, all functionalities are combined in one radio.

3G HF radios are GPS time synchronized, and radios in a HF network scan the same frequencies synchronously, giving very rapid linking. The waveforms used during link setup are 8-PSK modulated and encoded with Walsh functions, making the link procedure very robust at low SNR's. S4538 defines both Fast Link Setup (FLSU) and Robust Link Setup (RLSU). Only FSLU has been implemented in the RF-5800H from Harris.

In the Harris implementation, there is a direct IP interface at the radio, supporting both Ethernet and PPP, and making the radio act as an IP router.

The data link protocol xDL is defined for a point-to-point link, and it can further be divided into two classes of protocols called HDL (High throughput Data Link) and LDL (Low latency Data Link). HDL is optimized for delivering large datagrams in medium to good channel conditions and LDL is optimized for delivering small datagrams in all channel conditions and also longer datagrams in poor channel conditions. The different performance of HDL and LDL under various channel conditions is caused by the characteristics of the different burst waveforms used. Both protocols employ ARQ and code combining for adaption of data rate to channel conditions.

The maximum gross data rate of the waveforms in S4538 (Edition 1) is 4800 bits/s. The throughput of the data link protocol using ARQ will be less. There is a finite number of forward transmission frame sizes of the data link protocol, limiting the throughput efficiency.

xDL offers a point-to-point service for both circuit and packet switched data. There is also a point-to-multipoint (multicast) service defined for circuit switched data, but not for packet switched data. Harris has however, implemented a broadcast packet service in the RF-5800H.

4 HDL+ DATA LINK PROTOCOL

The current version of S4538 (Edition 1), includes waveforms with a relatively low maximum gross data rate (4800 bits/s). In a future edition of the standard, a new data link protocol providing higher throughput has been proposed and will be incorporated. The protocol has been designed to support an efficient exchange of IP based data traffic. Harris Corp has developed and implemented this data link protocol called HDL+ [8].

The basic ideas of the protocol are to combine the high data rate waveforms of S4539 with some code combining technique, and also make the size of the forward transmission frames more flexible. This enhances the adaptivity and flexibility of the data link protocol compared to xDL in S4538, and the theoretically maximum throughput of HDL+ can be ~10 kbit/s. HDL+ gives a significant higher throughput than the current S4538 at high SNR's and benign channels. For low SNR's and difficult channels, the HDL+ protocol has no potential gain compared to the xDL protocols in S4538, and the Harris implementation resorts to xDL.

The same 3G link setup defined in S4538 is used for xDL and HDL+.

5 IMPLEMENTATION ISSUES

There are a number of radio implementation choices that influences our performance measurements.

The Automatic Channel Selection (ACS) algorithm does not affect interoperability and is therefore not standardized. However, the ranking of frequencies and the following selection of frequency to link on, has great impact on the measured throughput, particularly when channel conditions are difficult.

The data rate adaption algorithm and the corresponding selection of appropriate waveforms is also of great importance to the measured throughput. For instance, holding on to a non-robust waveform when channel conditions have deteriorated, decreases the measured throughput.

There is also an implementation trade-off between allowing for maximum throughput in one direction or traffic flow in both directions. This will also influence measured throughput, depending on measurement method.

In [6] we addressed the problem of a data source generating packet data at a high rate, higher than what can be supported by the HF link. When there is no mechanism for flow control as in our case using UDP/IP (next section), the buffer of the radio at the transmitter will overflow and subsequent packets will be discarded. However, both the Harris RF-5800H and the Thales XOmail product have implemented the Source Quench Message of the IP Control Message Protocol (ICMP), which reduces the data flow from the source. This will reduce the effect of buffer overflow, but nevertheless cause a non-optimal utilization of the link protocol. This situation will reduce the measured throughput, and in our case occurs at file sizes greater than 10 kbyte.

6 MILITARY MESSAGE HANDLING SYSTEM (MMHS)

For exploring the capabilities of a 2G and 3G HF system we have used a NATO standardized application; the Military Message Handling System (MMHS) described in STANAG 4406. In NATO, formal messaging is seen as the vehicle for secure, mission critical, operational, military applications, and e-mail systems are not. STANAG 4406 includes both a connection-oriented protocol stack suitable for strategic high data-rate networks (Annex-C) and a connectionless protocol stack suitable for tactical low data rate connections (Annex-E). Thus, a common baseline protocol solution exists so that MMHS can be used in both the strategic and tactical environments.

Over an HF link the tactical protocol stack in Annex-E obviously must be used. In addition to being connectionless which gives less overhead and avoids the large turn-around times of the link, compression is used, and there is a choice of full-duplex, half-duplex or simplex operation. It may also be used for both unicast and multicast, the latter providing efficient use of radio resources. There are also procedures for handling recipients under Emission Control (EMCON).

Since the Annex-E protocol profile uses a connectionless transport service, there is no inherent transfer reliability. This is compensated for by the introduction of the P-Mul sublayer. The P-Mul protocol is defined by the military standard ACP 142 [ref]. This sublayer has functionality for both unicasting and multicasting of messages. It splits the message into smaller Protocol Data Units (PDU's), attaches a checksum, numbers the PDU's and handles retransmissions based on a selective repeat procedure. Since the P-Mul protocol supports retransmissions of lost packets, the bearer service does not need to be reliable (i.e. broadcast). However, both the 2G and 3G HF systems were run in ARQ-mode in our tests, providing a reliable service to the application.

A connectionless WAP transport protocol called the Wireless Datagram Protocol (WDP) is specified in Annex-E. This protocol is more flexible than the UDP protocol in that it does not mandate the use of IP. If IP is used however, the WDP protocol becomes UDP. In our tests where the HF radio provides an IP service, Annex-E uses the UDP protocol, and the traffic flow is essentially unidirectional over the HF circuit.

7 MEASUREMENTS

The performance of the HF protocols was evaluated by testing in controlled lab environments as well as by on-air measurements. The lab testing was limited to AWGN channels. All testing reported in this paper is performed with IP traffic generated according to STANAG 4406 Annex E implemented in the XOmail product from Thales.

The practical test-setup for 2G testing and 3G/HDL+ testing was slightly different, reflecting only differences in the practical implementation of the two protocols as described above. The test setups are shown in Figure 1 for the 3G/HDL+ testing (left) and 2G testing (right).

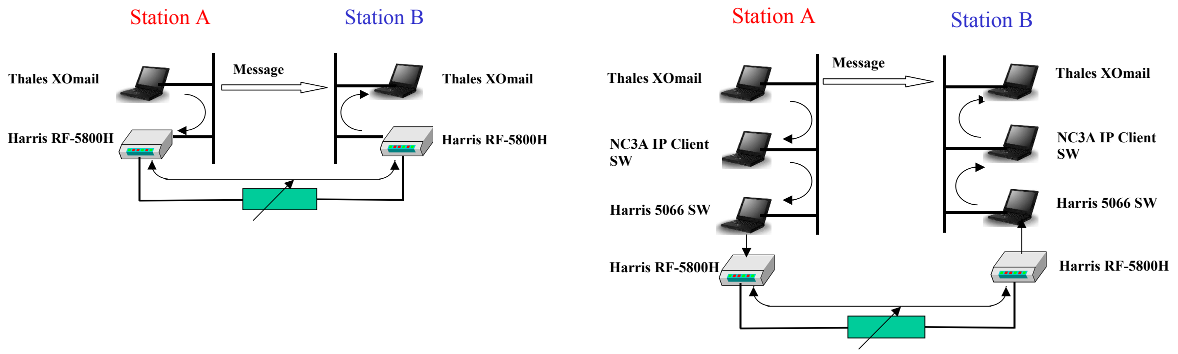

Figure 1 Test setup for MMHS over a 3G HF system (left) and a 2G system (right)

The measurements were made by observing the transfer times of XOmail messages when repeatedly transmitting compressed messages with a known compressed message length L. Thereby, an estimate of the mean transfer time for all the repetitions T_{mean} could be calculated. The instantaneous throughput of the message repetition i is defined as $G_i = L/T_i$, where T_i is the transfer time of the specific repetition. Likewise, the mean throughput for all repetitions is defined as $G_{mean} = L/T_{mean}$. The number of repetitions of a measurement series was normally 10, except in situations with very high transfer times or when particular conditions prevailed. Each new transmitted message was released only after the previous ALE session was fully terminated, necessitating a new automatic link establishment. Hence ALE setup times are included in the measured transfer times and in the throughput calculations. A pool of 10 different frequencies defined the HF net.

From the definitions above, it is noted that the throughput figures in this paper relate to the application throughput, i.e. the average number of compressed application data bits transferred per seconds. The throughput of the HF link will be higher, because of the overhead introduced by the XOmail application and the overhead of the UDP/IP packets. For the configuration of XOmail used during the measurements, the relationship between the throughput of the HF link and the application throughput can be approximately expressed as:

$$G_{link} \approx G_{appl}*(1{,}0887 + 700/L) \qquad (1)$$

where G_{link} and G_{appl} is the throughput at the link level and the throughput at the application (message) level respectively, and L is the length of a compressed message.

The measured transfer times depend upon the standardized protocols as well as radio implementation choices, as mentioned earlier. In addition, the transfer times are impacted also by the traffic characteristics and the protocols of the application, such as the rate of arrival of IP packets at the radio and the size of the IP packets. The latter parameters were fixed within a suitable range and kept constant during all the measurements.

7.1 MEASUREMENTS AND COMPARISONS IN THE LAB

The protocols were explored in the laboratory using the block schematics of Figure 1, with the additional insertion of additive white Gaussian noise at a controlled level at the inputs of each radio. The measurements consisted of two parts. First, the protocols were tested under “ideal” channel conditions with different message lengths. During these measurements the SNR was set to about 37 dB, making use of the highest speed waveforms technically feasible. All 10 frequencies were operated with the same SNR, thus eliminating the importance of the channel selection algorithms.

Secondly, the throughput was measured as a function of the SNR, keeping the message length constant. The SNR was identical at both ends of the link.

Figure 2 (left) shows how the average throughput on an “ideal” channel varies with the message length for the three different HF protocols. The 3G protocol offers less throughput than 2G for large message sizes. This is because the 3G waveforms offer a lower maximum data rate than the waveforms of 2G. The HDL+ protocol performance is superior to that of 3G for all message lengths. It is noted that a slight reduction in the application throughput performance for the HDL+ and the 3G protocols occurs for messages larger than 10 kbyte. This is a consequence of buffer overflow in the radio and the impact of the Source Quench message on the packet flow from the XOmail application. The effect is not visible for the 2G protocols because the traffic from XOmail enters into the NC3A IP client software (Figure 1). The latter has a large enough buffer capacity to avoid overflow for the message sizes used in these tests.

The reason for the poor throughput performance of the 2G for low to moderate message length is the slow automatic link establishment of the 2G system. The throughput of the 2G protocol will improve significantly for these message lengths in the absence of ALE.

Figure 2 (right) also shows the measured throughput performance of the protocols as a function of the SNR on an AWGN channel. The compressed message length is 9.3 kbyte. For positive SNRs the HDL+ protocol gives a superior performance, justifying a revision of the STANAG 4538. However, for low SNRs the performance of the HDL+ and the 3G protocols was similar. This is according to expectations, since the two protocols use the same waveforms for low SNRs. The long linking time of the ALE protocol in the 2G HF system prevents its throughput performance to approach that of the 3G protocol at positive SNRs, and its low robustness prevents any message transfer at all for the lowest SNRs.

The link level throughput will be about 16% higher than those shown in Figure 2, as given by equation (1). Even at SNRs approaching 30 dB the link throughput of the lab tests of HDL+ is less than half the throughput figures reported in [8] for a 5 kbyte message. This is not the case for the 3G results from [8], which is in better accordance with the results of Figure 2. The reasons for this discrepancy for the HDL+ protocol are not fully understood, however, it might be related to implementation effects of the HDL+ protocol and to the arrival rate of IP packets from the message source not satisfying the conditions for maximum throughput.

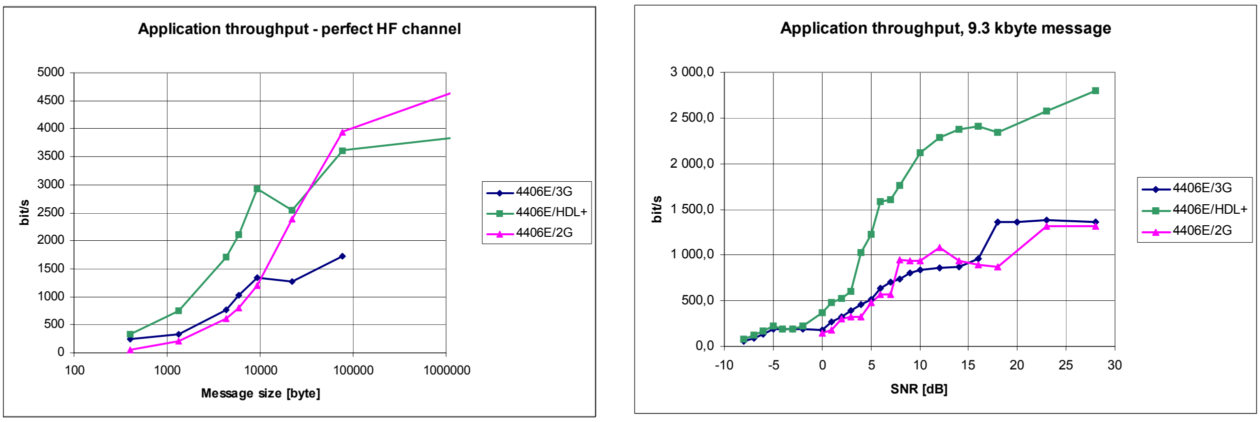

Figure 2 *Comparison of throughput versus message size (left) and comparison of throughput versus SNR for a 9 kbyte message (right) for 2G, 3G HF and HDL+*

7.2 MEASUREMENTS AND COMPARISONS OVER-THE-AIR

The comparative testing of the three protocols proceeded by measuring the throughput performance of a HF link between Lillehammer and Kjeller in southern Norway. This link is believed to be fairly representative of a tactical NVIS link between vehicular equipments; the distance being approximately 140 km and the transmit power being 125 W.

Measurements were conducted in March/April 2004 mostly under benign conditions, the local geomagnetic K index was never above 3 for the data shown in this paper. The noise level at Kjeller was particularly high during daytime causing the SNR to be 10-15 dB lower than at Lillehammer. Lilehammer was therefore chosen as receive site for all the measurements.

The same pool of 10 frequencies was used during all measurements. In order to compare the protocol performance, the protocols were tested in sequence during a sub-period as illustrated in Figure 3. Before the measurements of the message transfer times commence in each protocol measurement interval, there is a configuration phase. For each protocol, this phase also contained channel soundings, so that the ACS algorithms can take advantage of up-to-date information on channel quality scores at the start of the measurement phase of each protocol.

After a number of independent message transfers with a given HF protocol, the mean throughput was calculated and used as the throughput estimate at the universal time corresponding to the middle of the observation interval. Also the minimum and the maximum instantaneous throughput values in the measurement interval were calculated.

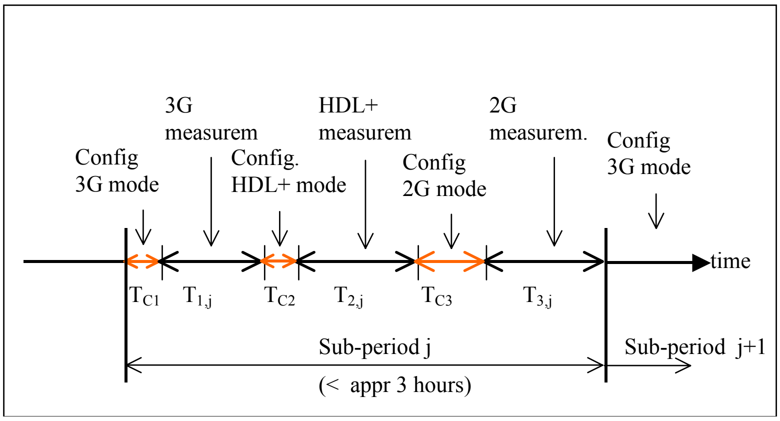

Figure 3 Test schedule of different protocols over-the-air

A message length of 9,3 kbyte has been used during most of the testing, and normally the number of repetitions of a message transfer was set to 10, resulting in a measurement interval per protocol of between 20 and 60 minutes. The variation of the message transfer times, and consequently the instantaneous throughput value, during each measurement interval could in some cases be significant. Not only the channel conditions seemed to contribute to this variation. Sometimes the ACS system would pick an unfortunate frequency, the effect of which was a sharp increase in the transfer time. This was more noticeable for the HDL+ measurements than for the measurements of the 3G and 2G system.

Figure 4 illustrates short-term variability of the HDL+ measurements by showing the average transfer time for each interval along with the maximum and the minimum transfer times measured during the 10 repetitions.

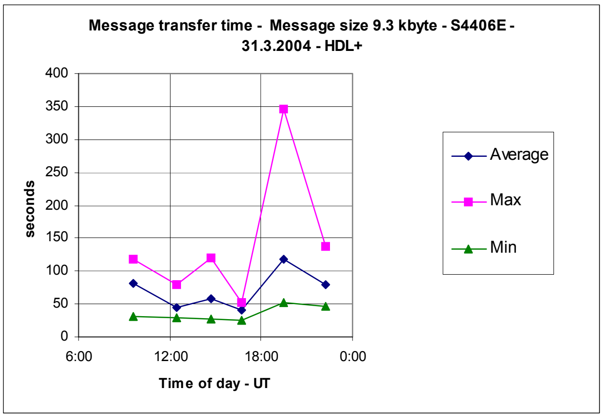

Figure 4 Short-term variability of the message transfer time of the HDL+ protocol

Figure 5 compares the average throughput for each measurement interval for the three protocols for the transfer of a 9,3 kbyte message (left) and a 22 kbyte message (right).

The results of the over-the-air testing confirm the impression that the HDL+ protocol offers an overall performance improvement for the transfer of short to medium length messages. However, it is noticed that under good day-time conditions with SNRs above 20 dB, the measured average throughput for the HDL+ remained well below the simulated throughput for a 5 kbyte message on an ITU Poor HF channel [8].

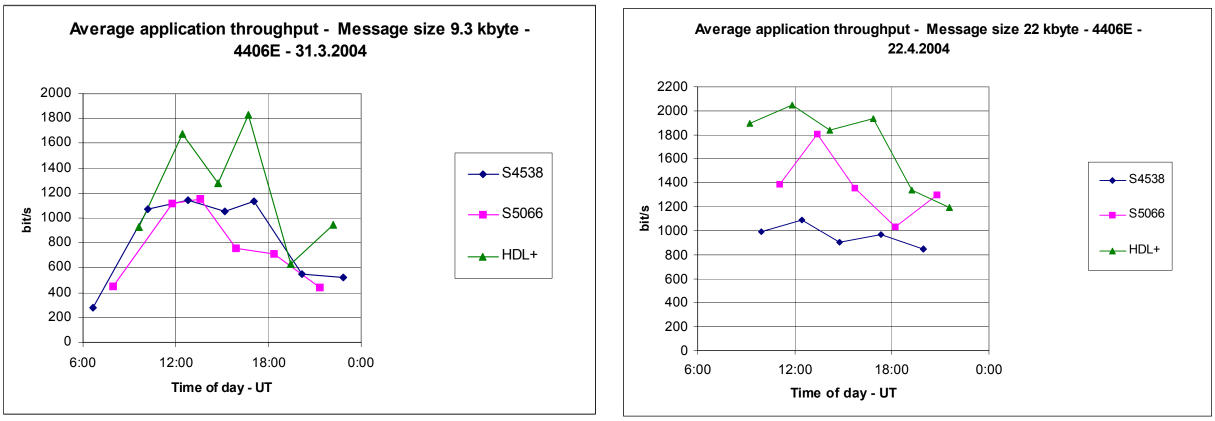

Figure 5 *Comparison of application throughput using the different HF protocols. 9 kbyte message (left) and 22 kbyte message (right)*

The difference between the measured performance between the HDL+ and 2G is primarily caused by to the less efficient linking protocols of the 2G.

It is expected that the message lengths in the tactical network in many cases will be much lower than 9 kbyte. Figure 6 compares a set of measured application throughput values for the HF protocols for message sizes of 403 byte, 1,3 kbyte and 9,3 kbyte. Each bar represents the average of 10 measurements. As expected, the throughput degrades rapidly as the message size is reduced, illustrating the fact that the HF protocols need to operate on large messages in order to achieve good throughput values.

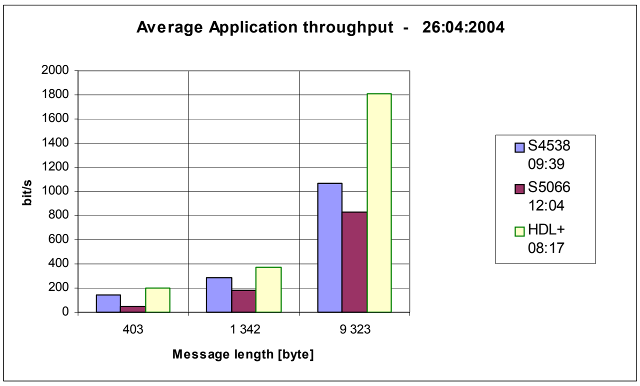

Figure 6 *Comparison of application throughput for various file sizes and HF protocols*

8 CONCLUSIONS

Testing a 2G and 3G HF system as part of an IP network using traffic from a STANAG 4406 Annex E message server has shown that the throughput of such a system can be lower than expected from knowledge of the optimum throughput capacity of the HF data link. This is related to the interaction between the offered load from the application and the HF data link protocols.

The linking used by the 2G HF system deteriorates the performance compared to the 3G system both in efficiency and robustness. This is particularly evident for small file sizes were the transmission time is short. The throughput of HDL+ is superior to that of 2G and 3G HF at positive SNR's. However, for larger file sizes (>22 kbyte) the performance of 2G approaches that of HDL+. At negative SNR's, 3G still provides communications whereas 2G fails to link. Implementation choices, such as ACS and the data rate adaption algorithm, have a great impact on the measured throughput.

ACKNOWLEDGEMENT

Thanks to Harris Corporation for technical support of this work.

REFERENCES

[1] NATO Standardization Agreement (STANAG) 4406, Military Message Handling System (MMHS), Ed. 1, 1999

[2] US Mil-Std-188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment, Appendix A

[3] NATO Standardization Agreement (STANAG) 5066, Profile for High Frequency (HF) Radio Data Communications, Version 1.2

[4] NATO Standardization Agreement (STANAG) 4539, Edition 1, Technical Standards for Non-Hopping HF Communications Waveforms

[5] NATO Standardization Agreement (STANAG) 4538, Edition 1, Technical Standards for an Automatic Radio Control System (ARCS) for HF Communications Links

[6] Jodalen V, B Solberg, A Eggen, A B Leere, O K Grønnerud, "IP over HF as a bearer service for NATO formal messages", *IEE Conference Publication No 493,* Ninth International Conference on HF Radio Systems and Techniques, pp 19-24, Bath, UK, 2003

[7] Smaal J W, Application Note: STANAG 5066 IP Subnet Client, SISmcast, NC3A, http://elayne.nc3a.nato.int

[8] Chamberlain M W, Furman W N, HF Data Link Protocol Enhancements based on STANAG 4538 and STANAG 4539, Providing Greater than 10 kbps Throughput over 3 kHz channels, *IEE Conference Publication No 493,* pp 64-68, Bath, UK, 2003

[9] Allied Communication Publication (ACP) 142 v 1.0, P-Mul: An Application for Multicast Messaging under EMCON Restriction, 2000

D APPENDIX

NATO MILITARY MESSAGING IN THE TACTICAL DOMAIN – PERFORMANCE ISSUES OF AN HF CHANNEL

NATO Military Messaging in the Tactical Domain –performance issues of an HF channel

Vivianne Jodalen, Anders Eggen, Bjørn Solberg and Ove Grønnerud
Norwegian Defence Research Establishment (FFI)
P.O. Box 25
N-2027 Kjeller, Norway

E-mail: vjo@ffi.no, ane@ffi.no, bso@ffi.no, okg@ffi.no

SUMMARY

NATO STANAG 4406 for Military Message Handling Systems (MMHS) may be used for direct information exchange between the high data rate strategic domain and the low data rate tactical domain by using the tactical protocol profile specified in Annex E. This paper explores the performance of the MMHS application over NATO standardized HF radio systems using both unicast and multicast IP services. A comparison of performance is made with a dedicated HF messaging application, and advantages/disadvantages by using the IP based application are pointed out. MMHS Annex E over HF systems is a viable solution, providing application throughputs up to a few kilobits per second. There are however, optimisation issues at different levels of the protocol stack, and we have seen that implementation choices and parameter settings have great impact on the overall performance of the system.

1.0 INTRODUCTION

Interoperability between communications equipment used by military forces from different countries is very important in todays battlefields. During the last ten years NATO has produced a number of standards (STANAGs) for military information systems, ranging from applications to bearer services such as HF communications. Using standardized protocols at all levels of the protocol stack provides interoperability and flexibility. IP will be the integrating networking technology in future military communications network, and many nations are planning to use IP as a platform for their communication systems in both the strategic and tactical domains. This will provide increased interoperability between strategic and tactical systems. However, there may be challenges when the TCP/IP protocol suite is used over tactical communication systems with variable quality and data rate. Traditionally for tactical communication systems, applications have been uniquely tailored to the bearer service. This provides efficient utilization of the channel capacity, but at the cost of flexibility and re-use of the same applications.

This paper describes the exploration in the lab and over-the-air of a NATO standardized application; the Military Message Handling System (MMHS) specified in STANAG 4406, used together with NATO standardized HF communication systems specified in STANAG 4538 (3G HF) and STANAG 5066 (2G HF). A new HF datalink protocol (HDL+) proposed for standardisation, is also included in the evaluation. STANAG 4406 for MMHS includes both a strategic and a tactical protocol profile, which may be used for exchanging information between the high data rate strategic domains and the low data rate tactical domain. We discuss the use of IP as an integrator between the MMHS application and the HF bearer services. The MMHS may also be used as an integrator between tactical bearer systems such as HF/VHF/UHF/WLAN.

In NATO Network Enabled Capabilities (NNEC) seamless interconnection of systems and networks is an

V. Jodalen, A. Eggen, B. Solberg, O. Grønnerud (2005) NATO Military Messaging in the Tactical Domain - performance issues of an HF channel. In *Military Communications* (pp. 11-1 – 11-16). Meeting Proceedings RTO-MP-IST-054, paper 11. Neuilly-sur-Seine, France: RTO. Available from:

important factor. In the migration process towards NNEC, we believe the MMHS based on STANAG 4406 may be used as an integrator between strategic and tactical systems because most NATO nations (including the NATO organization) recently have procured systems in accordance with this standard.

2.0 NATO MILITARY MESSAGING

A Formal Military Message is different from an interpersonal message in that it is a message sent on behalf of an organization, and that it establishes a legal commitment on the sending and receiving organization under military law. Examples of formal messages are military orders.

Formal Military Messages are handled by Military Message Handling Systems (MMHSs). An MMHS takes responsibility for the delivery, formal audit, archiving, numbering, release, emission, security and distribution of received formal messages. In NATO, the formal messaging service is seen as the vehicle for secure, mission critical, operational, military applications (e-mail systems are not). STANAG 4406 Ed.1[1] [1] is the only agreed standard to achieve interoperability between the formal messaging systems of NATO nations. Systems compatible with the S4406 standard have been and are being implemented widely by the NATO nations and by the NATO organization.

2.1 Military Messaging in the tactical domain

The original connection oriented protocol stack defined in S4406 Annex C (and ACP 123 [2]) was developed for strategic high data rate networks, and is not suitable for channels with low data rate. A protocol solution defined in Annex E of S4406 has therefore been developed for *tactical* communications. With the inclusion of this protocol profile in S4406, a common baseline protocol solution exists that opens for a seamless interconnection of MMHS between the strategic (fixed) and tactical (mobile) environments. One messaging system may therefore be used to communicate with all national forces, the NATO organization and the NATO allies. In Figure 1 the MTA (Message Transfer Agent) may be used as a gateway between the strategic and tactical domain if the dual stack is implemented.

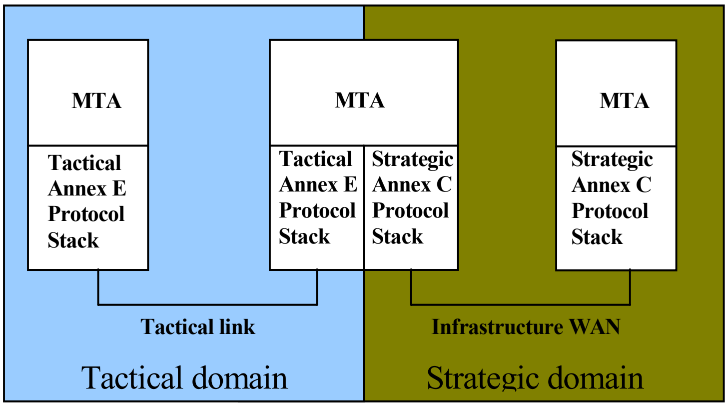

Figure 1: Seamless interconnection of MMHS between the strategic and tactical domain

To take account of the characteristics of a tactical radio link, the Annex E protocol profile has adopted the following:

---

[1] STANAG 4406 Edition 2 is out for NATO ratification at the time of writing.

- A connectionless protocol stack, which gives less overhead and reduces the effect of large turn-around times of the link
- A choice of full-duplex, half-duplex or simplex (broadcast) operation
- Compression to reduce the amount of data transmitted
- It may be used for both Unicast and Multicast, the latter providing efficient use of radio resources
- Procedures for handling EMCON recipients

The protocol profile in Annex E is divided into an application layer and a transport layer on top of potential bearer systems. Among several sub-layers, the P-Mul protocol (ACP-142 [3]) is introduced to compensate for the lack of transfer reliability of the connectionless protocol stack. It splits the message into smaller Protocol Data Units (PDU's), attaches a checksum, numbers the PDU's and handles retransmissions based on a selective repeat procedure. The P-Mul sub-layer has also functionality for both multicasting and unicasting of messages. The transport layer of Annex E uses a connectionless WAP protocol called the Wireless Datagram Protocol (WDP). This protocol is more flexible than the UDP protocol in that it does not mandate the use of IP. However, for IP networks the WDP protocol becomes UDP. In our test where the HF radio provides an IP service, Annex E uses the UDP protocol.

These features of Annex E increase the messaging throughput substantially for tactical communication channels with low data rate compared to the connection oriented Annex C protocols. We have used the Thales XOmail implementation of S4406 in our tests, including both the tactical (Annex E) and strategical (Annex C) protocol profiles.

3.0 TACTICAL RADIO COMMUNICATIONS

Tactical communications are used by highly mobile units not being able to utilize a fixed communications infrastructure. Typical tactical units requiring long range tactical communications are: Naval vessels, aircrafts, land mobiles and special forces carrying manpack radios. The characteristics of long range tactical radio communications in general are:

- Only low to moderate data rate is supported (typically < 10 kbit/s)
- Variable data rate depending on time, location and other users of the radio spectrum
- Unreliable connections; high bit error rates, frequent link terminations, unreachable nodes, equipment failure
- Half duplex or simplex channels, giving large turn-around times
- Different types of radio equipment
- Emission Control (radio silence) conditions are often required

3.1 NATO HF Communications

The above characteristics apply to HF communications in particular, since HF propagates via reflecting layers of the ionosphere that supports a very limited data rate. Under very favourable conditions, a maximum of 9.6 kbit/s user data rate can be achieved in a 3 kHz channel. However, the data rate is normally much lower due to absorption of the signal, manmade noise and interference. Also, rapid time fading and excessive multipath impose a reduced data rate. HF radio systems normally operate in half duplex mode. The advantage of HF communications is extraordinary radio coverage well beyond line-of-sight.

NATO has developed a family of standards at the physical and data link layer within the "HF House" concept. The HF House covers what is called 2G HF technology and 3G HF technology, both of which contain descriptions on *automated* procedures at the link level, appropriate waveforms to be used at the physical level and how the HF subnetwork can interface a data network. Our tests described in this paper have included both 2G and 3G HF technology and also a new data link protocol (HDL+) that will be standardized in the near future. The most important characteristics of the respective HF technologies are described in the following sections.

3.1.1 2G HF

A common operational configuration of a 2G HF system is based on the following set of HF standards: Mil-Std 188 141A [4], STANAG 5066[5], and STANAG 4539 [6]. Mil-Std 188 141A provides automatic link establishment (ALE) in a net of HF radios scanning asynchronously. The link set up may take some time depending on the number of frequencies in the scan set. The waveform used for linking is not particularly robust at low signal-to-noise ratios. When a link is established, the data link protocol defined in S5066 provides efficient and reliable data delivery on a point-to-point link using Automatic Repeat Request (ARQ) and appropriate waveforms defined in S4539. The ARQ scheme is used for adapting the data rate to the channel conditions. The gross data rates provided by the waveforms in S4539 range from 75 bit/s to 9.6 kbit/s. The data link protocol can also be run in broadcast mode where no feedback is provided from the receivers. This does not give a reliable delivery service and eliminates the mechanisms for adapting the data rate.

S5066 defines a subnetwork service interface that consists of a number of service access points (SAP's), including a SAP for IP. IP datagrams must be included in service primitives before delivery over the SAP to the data link protocol. The conversion between IP datagrams and S5066 service primitives is handled by a separate software package, in our case the IP Client software delivered from NC3A [7]. Other SAP's defined in S5066 provide an efficient interface to other applications, for instance HF mail applications such as HMTP and CFTP, without any intervening transport and networking protocols such as UDP/TCP/IP.

For the standards defined above we used the Harris implementation in their RF-5800H radio product and the Harris WMT S5066 software package.

3.1.2 3G HF

For 3G HF, STANAG 4538 [8] includes all the functionalities such as link setup, data link protocol and waveforms. The link setup defined in S4538 is based on all radios scanning a set of frequencies synchronously. The fast link setup (FSLU) used in our tests gives very rapid linking. The waveforms used for link setup are also very robust, enabling linking at negative signal-to-noise ratios. The data link protocol xDL is defined for a point-to-point link and gives an adaptive and reliable data delivery using ARQ and code combining. It is further divided into two classes of protocols called HDL (High throughput Data Link) and LDL (Low latency Data Link). HDL is optimised for delivering large datagrams in medium to good channel conditions and LDL is optimised for delivering small datagrams in all channel conditions and also longer datagrams in poor channel conditions. HDL and LDL use different waveforms with different robustness. The maximum gross data rate for xDL is limited to 4.8 kbit/s, which limits the throughput performance compared to 2G HF. All of the described functionalities of S4538 are implement in the RF-5800H from Harris used in our tests.

S4538 does not currently define a multicast/broadcast mode for packet data. However, the Harris RF-5800H radio provides a proprietary broadcast packet service where the data rate is fixed.

No subnetwork service interface is currently described in S4538. In the Harris implementation, there is a direct IP interface at the radio, supporting both Ethernet and PPP, and making the radio act as an IP router.

Applications using IP services may therefore connect directly to the radio.

3.1.3 The new data link protocol HDL+

A new data link protocol has been proposed by Harris to become a part of S4538 in the future. HDL+ is a point-to-point protocol and will to a large extent replace HDL, providing higher throughput and lower latency on good HF channels. The protocol has been designed to remove the data rate limitation of S4538 and to support an efficient exchange of IP based data traffic. The same efficient link setup is used for HDL+ as for 3G HF. The data link protocol combines the high data rate waveforms of S4539 with some code combining technique, and gives an adaptive data link protocol capable of error free delivery up to 10 kbit/s in a 3 kHz channel [9]. For poor channels the HDL+ has no potential gain compared to the LDL protocol in S4538, and the Harris implementation resorts to LDL. The same IP interface as for 3G applies to the HDL+ protocol.

3.2 IP over HF

The communications scenario we discuss in most of this paper is described in Figure 2. An HF link is used to connect the IP networks A and B. Two data terminals are hosting a S4406 Message Transfer Agent for provision of a seamless MMHS service to the mobile platform. The nodes HF A and HF B each comprise the HF radio/modem functionality, the HF link protocols, an optional link crypto functionality and finally an IP routing functionality.

Compared to most other links used in an IP network, the throughput of a typical HF link will be very low and variable, and the latency will be very high. In order to take advantage of the IP service offered by the HF radio link, the protocols above the network layer must be able to tolerate the high latency imposed by the HF link protocols. TCP is not particularly suitable for use over HF because of the variable capacity of HF requiring conservative timer settings and because the cost of reversing the channel at HF is rather high. In most cases the HF link will inevitably represent a bottleneck in the IP network with a great impact on the quality of service being offered to the user.

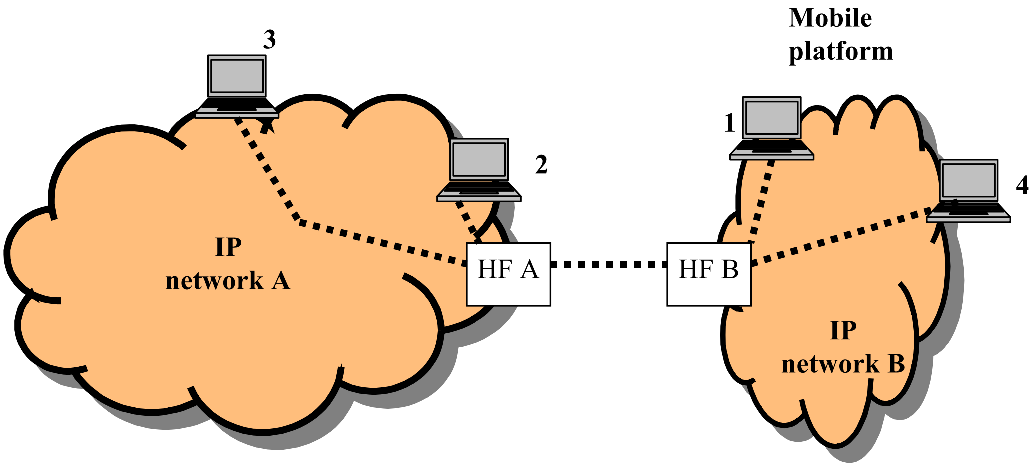

Figure 2: Model of IP networks connected by HF

4.0 PERFORMANCE OF THE NATO MESSAGING APPLICATION OVER HF LINKS

The aim of this study has been to explore the efficiency of the message transfer of the MMHS by using a transparent IP service over the different HF technologies and to understand the interactions between the protocols. Focus has been on efficiency over a point-to-point link, and measurements have been conducted in both the laboratory and over-the-air. Earlier published results can be found in [10], [11] and [12]. We have also addressed the Multicast properties of S4406 Annex E utilizing the Harris proprietary Broadcast protocol of RF-5800H. Laboratory measurements illustrate a few points about the efficiency of Multicasting over HF.

4.1 Recapitulation of earlier published results

Our first investigations were conducted in the lab under controlled channel conditions. The test setup was similar to the setup shown in Figure 3, except that the radios were connected with attenuators, and there was no need for a modem to control one of the radios. White Gaussian noise was inserted at a controlled level at the inputs of each radio, but no fading model was used. A frequency set consisting of ten frequencies has been used throughout the tests.

Figure 3 shows the test setup for the over-the-air tests that were conducted between Lillehammer and FFI at Kjeller, a 140 km path in southern Norway. A modem over the telephone network enabled us to control and monitor the message reception at the remote site, and transfer times were recorded. The power transmitted was 125 W and the antennas were broadband dipoles.

Thales XOmail (S4406) was located at the PC's together with the WMT S5066 software. For the 2G tests, a second PC hosted the IP Client software on each side.

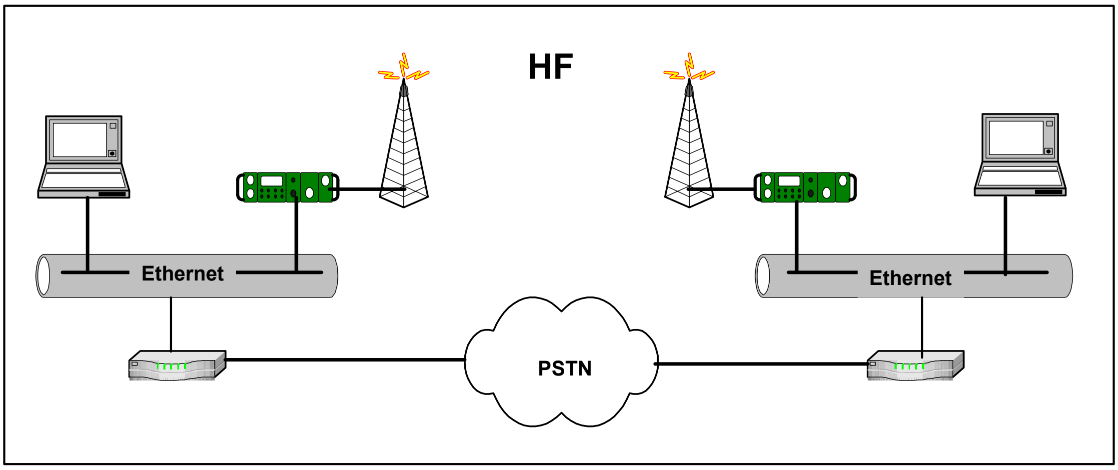

Figure 3: Over-the-air test setup

Compressed messages were transferred between the messaging application at each site, and the transfer times were recorded. The *application level throughput* was calculated as the compressed message size divided by the delivery time. Since the message is delivered before all the protocol layers have been released, the throughput calculations are slightly optimistic, in particular for short messages. Each measurement was repeated around 10 times and averaged. ALE/FLSU are included in the measured transfer times and in the throughput calculations.

4.1.1 Throughput

Comparing the througput performance on a “perfect” channel of the Annex C (strategic) and Annex E (tactical) protocol profile over S4538 (3G HF) shows that Annex E improves the throughput by a factor of six for a 400 byte file and by a factor of 2 for a 75 kbyte file. The improvement factor increases as the HF channel deteriorates, so that on a typical HF channel, the improvement factor will be higher than the figures mentioned here. In the following, only the Annex E protocol profile has been tested further since it outperforms the Annex C profile over an HF link.

We observed that transfer times (and therefore throughput) were affected not only by the protocols in use and the channel conditions. Also implementation choices made by the equipment vendors and configuration parameters selected by the user, contribute to the transfer times. For instance, the HF standards define a number of different waveforms, but the choice when to use the different waveforms is up to the vendor. Also frequency selection algorithms, buffer size and buffer handling are implementation dependant. Moreover, the transfer times depend on configurable parameters of the application such as PDU size and packet rate. Consequently, the throughput measured is only indicative of what can be obtained, and does not serve as a definite upper limit.

Our next observation focuses on the different HF link protocols (2G, 3G and HDL+) as the carriers of S4406 Annex E message traffic. We measured application throughput for various file sizes ranging from 400 bytes to 75 kbyte over an error-free channel. The results are shown in the leftmost panel of Figure 4. For message sizes below 10-20 kbyte, the HDL+ protocol gives twice as much throughput as the 3G and the 2G protocol. The 2G protocol suffers from in-efficient linking using Mil-Std 188 141A, and the 3G protocol suffers from low data rate waveforms. For larger message sizes (>20 kbyte) the effect of in-efficient linking for 2G is reduced and 2G performs at the same level as HDL+, but 3G still suffers from low rate waveforms. We will come back to the dip in throughput around message sizes of 20 kbyte for HDL+/3G in the next section. The rightmost panel of Figure 4 shows the application throughput versus signal-to-noise ratio on the channel for a fixed message size; 9.3 kbyte. At positive SNR’s the HDL+ protocol provides the best performance whereas HDL+ and 3G provides similar results at negative SNR’s. The 2G link establishment is less robust than 3G/HDL+, and linking is not achieved at negative SNR’s.

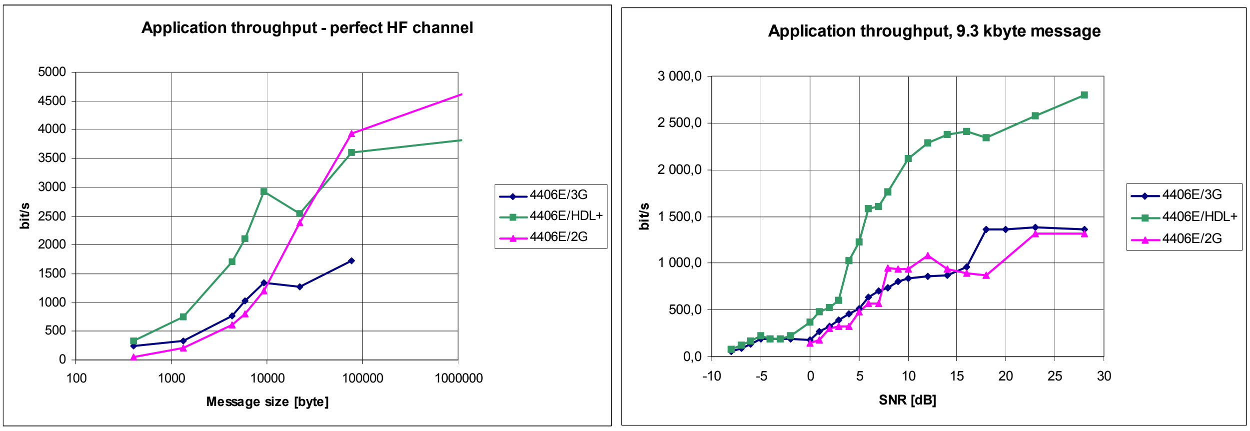

Figure 4: Comparison of throughput vs message size (left) and comparison of throughput vs SNR for a 9.3 kbyte message (right)

To compare the performance of the different HF protocols as bearers for S4406 traffic *over-the-air*, the protocols were tested in sequence but within a maximum time period of three hours. At the start of measurements for each protocol, channel quality scores in the radios were updated by channel soundings allowing an optimum frequency selection. Measurements were conducted in March/April 2004 under benign conditions, the local geomagnetic K index was never above 3 for the data shown in this paper.

However, the diurnal variability of the HF channel was quite noticeable. Figure 5 shows averaged application throughput vs time of day for a message size of 9.3 kbyte (left) and 22 kbyte (right).

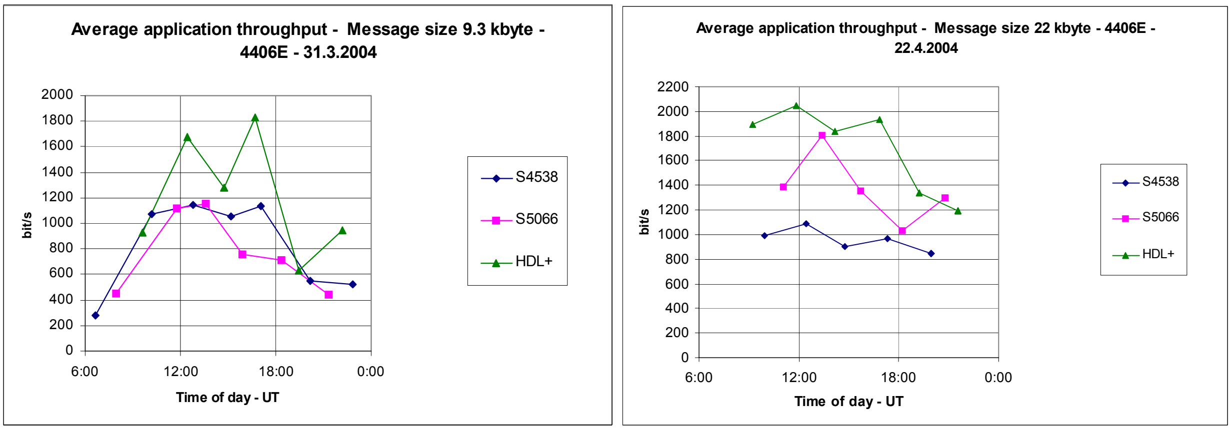

Figure 5: Comparison of throughput over-the-air vs time of day for a 9.3 kbyte message (left) and a 22 kbyte message (right)

The following conclusions can be drawn from the over-the-air tests of S4406 over the various HF protocols:

- Under good day time conditions (SNR > 20 dB) the measured average throughput for HDL+ remained well below the simulated throughput of 4500 bits/s for a 5 kbyte message on an ITU poor channel referred in [9]. Our results include the effect of non-optimum offered load from an application and realistic channel conditions which may be worse than the ITU poor channel.
- The variation of the message transfer times (and therefore throughput) when transmitting 10 consecutive messages for each HF protocol, is significant.
- The automatic channel selection algorithm of the radio is very important for achieving high throughput.
- The difference between the measured performance of the HDL+ protocol and 2G is primarily caused by the less efficient linking protocol of the 2G, and the effect of this is lower for larger message sizes.

4.1.2 Congestion control aspects

Referring to Figure 2, IP packets may arrive at the HF transmit node at a higher rate than the node is able to support, and hence, packets will accumulate in buffers at the HF node. With respect to the throughput of the HF link this is desirable, because the HF protocol efficiency improves with full radio buffers. However, since neither P-Mul nor UDP has mechanisms for network congestion control, buffers in the HF transmit node will tend to overflow, and packets will be discarded for long messages. The discarded packets will be retransmitted by P-Mul, but this effect may severely deteriorate the overall performance of the Annex E protocol stack.

The present XOmail implementation of ACP 142 P-Mul protocol and the IP service of the RF-5800H come around this problem by introducing a "local" congestion control mechanism, which makes use of the IETF standard "IP Control Message Protocol" (ICMP) (13). When the buffer of the HF transmit node overflows, an ICMP Source Quench message is generated and sent to the originating end terminal. This message will instantaneously stop the packet flow from P-Mul, thereby minimizing the influence of the buffer overflow. A timer will start the packet transmission again.

The buffer size of the RF-5800H in our 3G and HDL+ setups is about 10 kbyte. For message sizes exceeding the buffer size, a packet is discarded before the Source Quench is effectuated with a following reduction in throughput as seen in Figure 4 (left). The buffer size of the IP Client of the 2G HF subnetwork (software on a PC) is much higher, and no packets are discarded in the 2G measurements.

Although not perfect, by using the Source Quench mechanism for congestion control a reasonably high throughput capability will be achieved also when transferring long messages. However, there are unresolved issues regarding the use of the Source Quench mechanism. A new version of ACP 142 is under development by NATO and the CCEB, which will include functionality for end-to-end congestion control (see section 6.1).

4.2 Multicast

The broadcasting nature of radio nets can be utilized to offer an IP multicast service. This implies that IP data packets are broadcasted over the radio net and delivered to those addresses defined by the IP multicast address. In its simplest and most common form a multicast link service is based on broadcasting without link acknowledgements/retransmissions, and hence provides a less reliable service than unicasting. Multicasting may provide a potentially bandwidth efficient transfer capability, especially when there are many recipients of a message in the same radio network.

2G HF (S5066) offers a broadcast packet service. The 3G HF (S4538) in its present version does not. However, the implementation of S4538 from Harris that we are using in our tests, extends the present S4538 to provide a simple IP broadcasting service, on which a limited IP multicast service can be based. One of the key features of the STANAG 4406 Annex E is the multicast ability of the P-Mul protocol. We have done some introductionary testing to investigate how well this protocol will work on an HF network with S4538 extended with the IP broadcast protocol.

A multicast message transfer from A to three recipient nodes B – D has the following phases:

1. Transfer of the P-Mul Control PDU and the P-Mul traffic PDUs from A. Radio A sets up a channel on a suitable broadcast frequency and sends these PDUs by IP broadcasting at a fixed data rate.
2. Transfer of the P-Mul ACK/NACK control packets from each of the nodes B – D by using the S4538 unicast service.
3. Unless all the nodes have given a positive acknowledgement, P-Mul at node A will retransmit missing PDUs, and the nodes B – D will update their acknowledgement status. This repeats until all the nodes have received all PDUs from A.
4. When the P-Mul entity of node A has received acknowledgements from all the addressees, it will send an end-of-message (EOM) by IP broadcast, terminating the message transfer.

Thus, all P-Mul packets transmitted from node A use the IP multicast service, whilst the individual P-Mul ACK/NACK packets in the reverse direction use the unicast service. While the latter is a robust service with adaptable data rates and link acknowledgements, the former is a fixed data rate service without link acknowledgements. Hence the probability of delivery of a multicast message is strongly dependent on the fixed data rate selected for the channel. Unless a relatively low data rate is chosen for the broadcast channel, the IP multicast service will not be very effective in delivering messages to addressees that are operating on HF channels with low SNRs. For example, as a guideline, by using a data rate of 600 bit/s, HF channels with an SNR of a few dB's are required for acceptable delivery of multicast traffic. Increasing the rate to 4 800 bit/s increases the SNR requirements by about 10 dB.

Figure 6 shows a picture illustrating the difference in channel activity between the IP unicast service and the IP multicast service in the case of S4406 Annex E sending the same 2.5 kbyte message to 3 message recipients over an HF channel with an SNR of 6 dB. The IP broadcast data rate is 600 bit/s. The unicast service (left panel) handles the message transfer by sending the messages sequentially to one recipient at a time. The multicast message (right panel) is sent once and is delivered to all the recipients at the same time. The recipient nodes release their P-Mul acknowledgements approximately simultaneously, resulting in all three trying to set up a link to the originator at the same time and creating some havoc on the channel in this process. The S4538 protocol is able to resolve this channel allocation conflict, but it is noted that a very long time is spent for the transfer of the three ACK messages. In the end the originating node broadcasts an End of Message PDU terminating the P-Mul session.

The figure shows that in this given situation, less radio resources are needed when the IP multicast service is used to deliver the message. The message delivery time of the multicast message is about half of the average delivery time experienced when using three unicast messages. However, the P-Mul acknowledgement transfers taking place right after the multicast message delivery, are handled rather inefficiently by the protocols. The accumulated seizure time of the HF channel is still about 40% lower than for the unicast service in the above scenario, thus easing the load on the HF resources. This advantage will increase for an increasing number of message recipients. However, if the channel quality improves, the message transfer times for the unicast service will decrease because of the adaptive data rates, whereas the multicast service is stuck with the fixed data rate. This may change the picture of multicast using HF resources more effectively than unicast.

There are room for performance improvements for the handling of multicast traffic, as regards the implementation of the HF protocols as well as XOmail protocols. We believe that the use of S4406 Annex E combined with an efficient multicast link protocol has the potential of providing attractive solutions for several one-to-many HF communications scenarios.

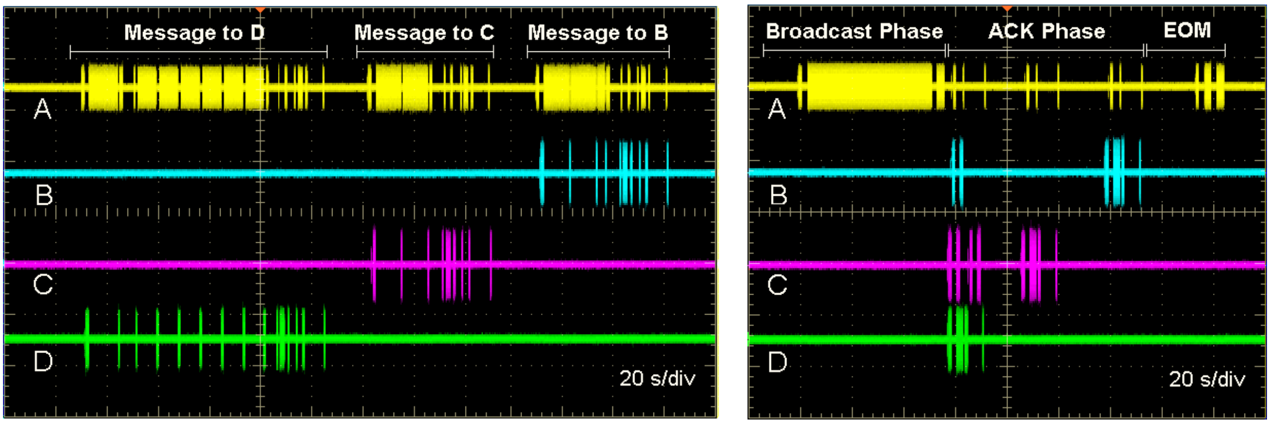

Figure 6. Oscilloscope traces showing the transmissions from the four HF radios when a message is sent to three destination addresses. The left/right panels show the activity when the message is sent as three unicast messages or as multicast, respectively. The upper trace represents the sending node.

5.0 A COMPARISON WITH A DEDICATED HF MESSAGING APPLICATION FOR UNICAST MESSAGE TRANSFER

The results presented so far are all based on the transparent transfer of IP packets carrying S4406 Annex E information wrapped in UDP PDUs over the HF links. There are, however, other options for transferring information over an HF link. As mentioned, S5066 defines a set of Service Access Points (SAP), some of which may be used to map the application information directly to the HF link level. Two of these are optional SAP's defined for use by the HF mail Transfer Protocol (HMTP) and the Compressed File Transport Protocol (CFTP), respectively. Both of these protocols are made for efficient packaging of messages for HF transfer. However, this solution of a direct mapping of the application information to the HF link layer does not provide any networking functionality. Consequently, such a solution is only viable over a one-hop HF link.

It would be reasonable that mapping application information directly to the HF link layer requires less HF capacity than if UDP/IP is involved. Hence it is to be expected that S4406 Annex E using a transparent IP service would be less efficient than using CFTP/HMTP mapped directly to HF. We used the Wireless Message Terminal RF-6710W (WMT) from Harris to send a message with a compressed attachment by CFTP over S4538, so that a comparison with XOmail using transparent IP over HF to send the identical message could be made. However, such a comparison is indeed a bit like comparing "apples and pears", since it does not account for the inherent advantages of the S4406 Annex E with respect to its offering of military services such as security and priority, or to the seamless interoperability it offers with military strategic messaging systems and with military procedures.

The following parameters were compared:

- the message delivery time.
- the total time duration that the HF channel is linked for the complete message transfer. This expresses the required use of HF resources for the message transfer.
- the number of bytes additional to the size of the compressed file that the S4538 has to transfer. This is a measure of how efficient the message is packaged at protocol levels above the datalink layer.

The measurements were made with a channel SNR of 20 dB. Figure 7 shows the measured performance parameters of S4406 Annex E (XOmail) using the transparent IP service over S4538 relative to the measured performance parameters of CFTP (WMT) mapped directly to the S4538 link protocol. It should be noted that the measurements do not only reflect the contributions from the standardized protocols, but are also affected by implementation choices and to some degree by processing times. One such important implementation parameter is the procedures and timer values used in conjunction with IP transfers over S4538. These are not part of S4538, and we believe there is some room for improvements in the efficiency of IP transfers of the measured equipment.

The green curve in the figure shows that the increase in the HF data link payload of the S4406 Annex E is very modest and only occurs for short messages. We assume that this increase may be at least partly explained by the added information that needs to be transferred due to the military services offered. The S4406 Annex E over IP also gives a slight increase of the message transfer time (blue curve). This percentage increase in transfer time grows with increased message size. This is primarily caused by the fact that the S4538 implementation organizes the IP traffic less efficiently than for bulk message transfer. The IP packets are organized in assemblies. Between each assembly there is a time gap in order to allow for channel reversal, and this time gap results in reduced protocol efficiency.

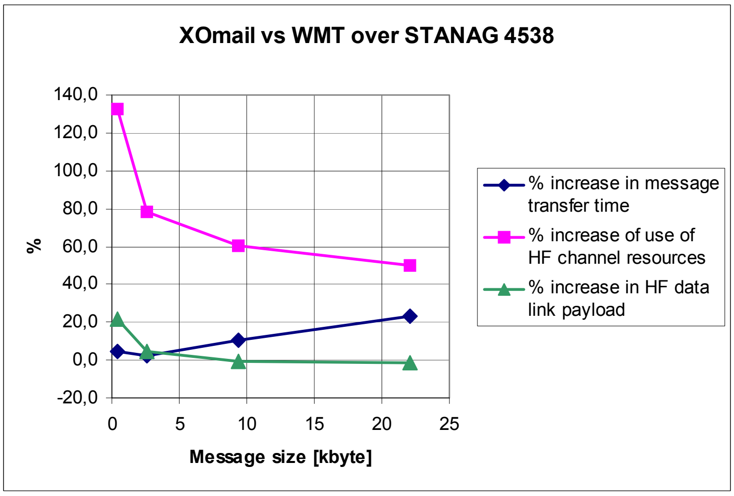

Figure 7. The performance of XOmail using a transparent IP service relative to using the WMT (CFTP) mapped directly to S4538.

The pink curve showing the most dramatic difference is related to the use of the HF resources, i.e the total time that the HF channel is occupied during one complete message transfer. There is a simple reason for this, which is the end-to-end acknowledgment mechanisms which are part of the Annex E protocol. The transmission of a P-Mul ACK in the reverse direction followed by a P-Mul EOM secures the S4406 Annex E message delivery reliability in an optimum manner. However, two channel reversals are necessary to accomplish this, and it is basically these channel reversals/HF link management messages that causes the use of the HF channel resources to increase sharper than the message transfer time. The WMT does not make use of a true end-to-end acknowledgement concept. It conveyed only the one-way message content on the HF channel.

The measured increase in message transfer time and the increased use of HF resources for the measured S4406 Annex E system are to a large extent attributable to its use of a transparent IP service and to the way that this service is handled by the implementation of the HF link protocol. Using the transparent IP service is a general solution, enabling HF to become an integrated part of the tactical internet. However, a solution with application data mapped directly down to the HF link layer will provide some efficiency gains. Such a gain may be provided also for S4406 Annex E systems, since there exists an option for a S4406 Annex E HF subnet interface SAP similar to those defined for CFTP/HMTP. As mentioned, the above comparison only considers the efficiency aspect of the message transfer. It must be kept in mind that important differences in functionality and service level between the systems are not reflected.

6.0 PROPOSALS FOR IMPROVEMENT OF THE P-MUL PROTOCOL (ACP 142)

We have experienced limitations of the current P-Mul protocol and implementation in our testing. A new version of ACP 142 is under development by NATO and the CCEB. Proposals have been made to include new functionality such as end-to-end congestion control, Forward Error Correction (FEC), handling of acknowledgement implosion and more dynamic mechanisms for adaptation of timers to the change in the communications conditions of disadvantaged grids. Since the proposals are still under discussion at the time of writing, some of the proposed functionality will be presented here without going into details.

6.1 Congestion control

In the current version 1.0 of the ACP 142 protocol, there are no congestion control mechanisms specified. The requirement for a congestion control mechanism and how it is solved using the IETF ICMP Source Quench protocol in the XOmail application and the RF-5800H radio is described in section 4.1.2. Since the congestion control problem is at the transmitting side between the application and the radio and not between the sending and receiving application, this form of congestion control is reasonable to use because it addresses the problems locally. However, because the ICMP Source Quench will not be maintained for IPv6, and the potential use of IP crypto will prevent the ICMP Source Quench packet from being transmitted from the radio to the application, another mechanism will have to be chosen. An end-to-end congestion control mechanism is being discussed for the next version of ACP 142. This solution will most likely be based on calculation of the measured delays of the P-Mul PDU's, which then will be used to regulate the flow of PDUs being sent from the P-Mul protocol. Timestamps may be added to some of the P-Mul PDUs in order to log the transfer time, which then is reported back to the sender. Such an end-to-end congestion control mechanism will not be as adaptable to the change in the communication conditions as the local ICMP Source Quench mechanism, because of the delay in getting the response. There are however, not many other alternatives if the use of IP crypto is not to be prevented.

6.2 FEC

An optional FEC mechanism in P-Mul is proposed. The main intention of the FEC is to improve the protocol performance on channels that are susceptible to PDU loss. This is the case when using radio channels with no acknowledgement mechanisms, for example when sending to EMCON recipients or when using a simple multicast protocol on a broadcast channel.

By introducing the FEC mechanism the complete message may be reconstructed by the recipient, even if a certain number of P-Mul PDUs are lost. This will increase the probability of message delivery to EMCON recipients. When using the multicast service with the FEC option, fewer (or no) negative acknowledgements will be required. In some cases, in particular when using HF protocols, the cost of returning an acknowledgment PDU may be high, and a reduction of the P-Mul traffic gives a noticeable performance improvement. On channels susceptible to PDU losses, a shorter delivery time is achievable by using the FEC option.

Reed-Solomon codes have been proposed as a suitable FEC mechanism at the P-Mul layer, due to its flexibility and its powerful error correcting capabilities.

6.3 More dynamic parameters for adaptation to the communication conditions

The current version 1.0 of the ACP 142 protocol uses static parameters that may cause problems when the protocol is used over radio systems with varying data rates end error conditions.

One of these static parameters is the re-transmission timer, which has to be set high if the condition of the channel is varying, in order to avoid premature time outs and retransmissions in the worst-case situations. A proposal has been made to make this timer more adaptable by taking into account the measured round trip delay and the size of the message to be transferred.

Another dynamic parameter proposed is the "Receiver Last PDU Timer". In the current version of the ACP 142 protocol, an acknowledgement is triggered by the reception of the last Data_PDU expected by the receiver. This means that if the last Data_PDU is lost, the receiver will not generate an acknowledgement. This will cause the transmitter to time-out and start re-transmitting the data. The new timer will trigger the generation of an acknowledgement if the last Data_PDU is lost, and will be calculated dynamically based on the arrival time of the previous Data_PDUs.

6.4 Handling Ack Implosion

If a message is multicasted to many recipients, there is a problem that the recipients may start sending acknowlegements at the same time. In radio networks, this may result in collisions because they all try to access the channel. In order to avoid this situation, there is a proposal for the next version of ACP 142 that all recipients are waiting a randomized period of time before sending the acknowledgement.

7.0 CONCLUSIONS

In the migration process towards NATO Network Enabled Capabilities, the MMHS based on STANAG 4406 may offer a seamless connectivity between NATO nations, between strategic and tactical units and between services. The MMHS is a tool for military command and control which, with the inclusion of Annex E, is extended to tactical users. The MMHS application may be used over different networking technologies and bearer services. By using the S4406 Annex E protocol profile we have shown that a reliable and reasonable message transfer is possible over an IP network which comprise an HF link. This opens for an architecture where the HF links may be directly utilized also for IP traffic from various other applications. This is not possible with mail applications dedicated for a specific radio link such as HF. However, the latter solution is able to utilize the HF channel resources more efficiently.

MMHS Annex E over HF systems is a viable solution, providing application throughputs up to a few kilobits per second. However, an HF link will represent a potential “bottleneck” in an IP network and it requires special attention for optimum performance. We experienced congestion control problems when using UDP/IP over a narrowband tactical link such as HF. Acceptable performance was achieved by using a congestion control mechanism based on ICMP Source Quench, but in the long term a new congestion control mechanism is called for.

The multicast functionality of S4406E promises to be an efficient way of delivering one-to-many traffic when used in conjunction with a suitable HF link service. In a simple one-to-many scenario tested, a significant reduction in the mean message delivery time was achieved and less radio resources were needed by transferring the message by an IP multicast service rather than by consecutive IP unicast transfers. The multicast performance can be enhanced further by modifications of the P-Mul protocol as well as in the RF-5800 IP broadcast protocol.

It is important to test complete systems together, ranging from application to the physical link. There are optimisation issues at different levels of the protocol stack, and we have seen that implementation choices and parameter setting have great impact on the overall performance of the system.

8.0 ACKNOWLEDGEMENTS

Thanks to Harris Corporation and Thales Norway, for technical support of this work.

9.0 REFERENCES

[1] NATO Standardization Agreement (STANAG) 4406, Military Message Handling System (MMHS), Ed. 1, 1999

[2] Allied Communication Publication (ACP) 123, Common Messaging Strategy and Procedures, Combined Communications Electronic Board (CCEB)

[3] Allied Communication Publication (ACP) 142 v 1.0, P-Mul: An application for Multicast Messaging under EMCON Restriction, 2000

[4] US Mil-Std 188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment, Appendix A

[5] NATO Standardization Agreement (STANAG) 5066, Profile for High Frequency (HF) Radio Data Communications, Version 1.2

[6] NATO Standardization Agreement (STANAG) 4539, Edition 1, Technical Standards for Non-hopping HF Communications Waveforms

[7] Smaal J W, Application Note: STANAG 5066 IP Subnet Client, SISmcast, NC3A, http://elayne.nc3a.nato.int

[8] NATO Standardization Agreement (STANAG) 4538, Edition 1, Technical Standards for an automatic Radio Control System (ARCS) for HF Communications Links

[9] Chamberlain M W, Furman W N, HF Data Link Protocol Enhancement based on STANAG 4538 and STANAG 4539, Providing Greater than 10 kbps Throughput over 3 kHz Channels, *IEE Conference Publication No 493,* pp 64-68, Bath, UK, 2003

[10] Jodalen V, Solberg B, Eggen A, Grønnerud O, IP over HF as a Bearer Service for NATO Formal Messages, *IEE Conference Publication No 493,* pp 19-24, Bath, UK, 2003

[11] Jodalen V, Eggen A, Solberg B, Grønnerud O, Military Messaging in IP Networks using HF Links, *IEEE Communications Magazine, Vol 42, No 11,* pp 98-104, Nov 2004

[12] Jodalen V, Solberg B, Grønnerud O, On-air Testing and Comparison of 2G and 3G HF, *Nordic HF Conference Proceedings,* p 3.5.1, Fårø, Sweden, 2004

[13] IETF RFC 792,"Internet Control Message Protocol (ICMP)"