FFI RAPPORT

PROTECTION OF NETWORK CENTRIC MILITARY RADIO COMMUNICATIONS

ÅSEN Walther, KÅRSTAD Jørn

FFI/RAPPORT-2004/02483

PROTECTION OF NETWORK CENTRIC MILITARY RADIO COMMUNICATIONS

ÅSEN Walther, KÅRSTAD Jørn

FFI/RAPPORT-2004/02483

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	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2004/02483	UNCLASSIFIED	12
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFI-II/832/113	-	

4) TITLE

PROTECTION OF NETWORK CENTRIC MILITARY RADIO COMMUNICATIONS

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

ÅSEN Walther, KÅRSTAD Jørn

6) DISTRIBUTION STATEMENT

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

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Radiocommunications	a) Radiokommunikasjon
b) Wave propagation	b) Radiobølgeutbredelse
c) Electronic Warfare	c) Elektronisk Krigføring
d) Network Centric Warfare	d) Nettverksbasert Forsvar
e)	e)

THESAURUS REFERENCE:

8) ABSTRACT

Protection of Network Centric Military Radio Communications depends on the ability to predict and counteract incidents that obstruct the networks' operation. This report gives a brief summary of the different effects that need be taken into account when constructing a computer programme that aims to optimise the network performance and predict probable problems.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
2004-08-02	Vidar S Andersen	Director

ISBN-82-464-0860-7

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

CONTENTS

PROTECTION OF NETWORK CENTRIC MILITARY RADIO COMMUNICATIONS

1 INTRODUCTION

Radio communications in a military setting means secure and reliable communications. Security is mainly achieved through cryptography, and is affordable, since it does not carry a bandwidth or power cost. Reliability, however, has a cost related to increased information bandwidth, increased transmission duration, increased transmission power requirements, or a combination of these factors.

The system architects' first problem is to decide how much information is to be conveyed between human-interface nodes in his network. This requires a thorough understanding of the operators' situations and needs. Beware that these requirements will vary strongly between functions and levels of the network. For some operators it suffices to receive simple signals or status alarms, while others need real-time video for conducting navigation or missile guidance. For making strategic decisions detailed imaging may also be needed, but in that case the information only needs to be timely, but not 'real time'.

Even though there is a clear understanding of all operative aspects, involving all possible operating theatres, there still remains the technical question of how much information bandwidth is really necessary in order to produce good user interfaces and operator positions. The answer to this question depends greatly on the capability to locally process data in the network. Soldiers on foot are not likely to carry heavy equipment for processing, and air platforms usually have restrictions on fitting electronic equipment. This means that raw data may need to be exchanged between units. Useful restrictions must therefore be set on areas of interest for the data streams passing through these human-interface nodes. Portable and lightweight equipment will most likely have reduced processing and transmission capability, which implies that they will be restricted to low-rate traffic, typically short message exchange.

When the restrictions on 'who gets what' are applied, the remaining issue is to deal with the radio-technical questions on how to relay information in an efficient manner, depending on the operating environment. The operating environment consists of several active parties; friends, neutrals, enemies and unknown. In addition there will be natural limitations related to topography, climate and short term weather conditions. The remaining part of this paper will describe a way to deal with these ingredients through use of the concept of a planning tool. The purpose of the planning tool is to protect your own Network Centric Military Radio Communications, taking advantage of all the information that you have available. The intention is to estimate the situation and the uncertainties, based on the information at hand.

Once the statistical distributions of estimated outcomes are known, the planning tool can accumulate the effects and calculate overall probabilities for each outcome. This can be used by the planner of the network to make risk based decisions. If no planning tool is used before deploying the network, the communication network will still be facing the consequences of some unfortunate moves, but then without a guess of the probabilities of the consequences occurring. In other words; if possible consequences of a set of moves and their respective chances are calculated beforehand, the decision maker will know his stakes.

2 A PLANNING TOOL FOR SUPPORT OF NETWORK CENTRIC WARFARE

The conceptual planning tool will consist of building blocks from different sciences and technologies. Signal processing in radio communications, wireless radio wave propagation, antenna theory, radio noise mapping, meteorology and mapping of meteorological phenomena, and communications Electronic Support Measures (sensing of communications traffic) will all be key elements. The intention is to use knowledge about these elements to make decisions under influence of the uncertainty that will dominate during hostilities, when the network is evolving dynamically. The dynamic aspect makes room for possible internal frequency conflicts in the network, which in itself is a reason for monitoring it closely.

The different building blocks of the network surveillance tool will now be discussed in more detail, focusing on effects that may be limiting to our planning tool, that is, effects that carry large statistical uncertainties.

Why do we want to quantify the distribution of these uncertainties? Primarily in order to answer questions like

- How do I organize my radio communications so that it is 99 % certain that they connect, 66 % certain that they are not intercepted by enemy communications ESM, and simultaneously 90 % certain that they cannot be jammed ?

- How can I employ my communication ESM units in order to make 99 % sure that they cover their mission?

- How can I obstruct the enemies' communications with 90 % certainty, and at the same time being 99 % certain not to kill my own communication links?

The planning tool will enable you to answer these and other probabilistically phrased questions.

2.1 Uncertainty related to radio wave propagation

The building block that carries the greatest uncertainty is probably models that predict how radio signals spread out from a radio emitter. These models depend on the topography, the climate and/ or the local weather.

At frequencies above about 1000 MHz communication requires ‘radio line-of-sight’, which means that any obstacle in the path may attenuate the signal enough to obstruct communication. At HF frequencies (3 MHz to 30 MHz) and below, the radio waves may in addition propagate through ionospheric reflections, and thus travel very far. So one may say that terrain in the path influences the signals in a smooth way at frequencies above 30 MHz and below 1000 MHz, but constitutes an absolute obstruction above this frequency. We may simplify and call propagation in this frequency domain ‘terrain limited’.

If no terrain obstructions are present, and we are using frequencies above 1 GHz, rain attenuation and absorption by atmospheric gases are the main factors limiting the propagation of radio waves. Molecular absorption is well described and can easily be calculated, and the uncertainty is thus mostly associated with rain or snow attenuation, which sets in at 8 GHz and above. We may again simplify and call this domain ‘precipitation limited’.

In the ‘terrain limited’ domain the uncertainty is associated mainly with the uncertainty of the terrain or building database. Typical standard deviations of height errors for digital terrain elevation data are in the order of 10 meters. These errors in height can be translated into errors in radio wave attenuation estimates, paying particular attention to the influence of the height errors close to the receiver and emitter antennas, using for instance the Okumura-Hata height correction term (1).

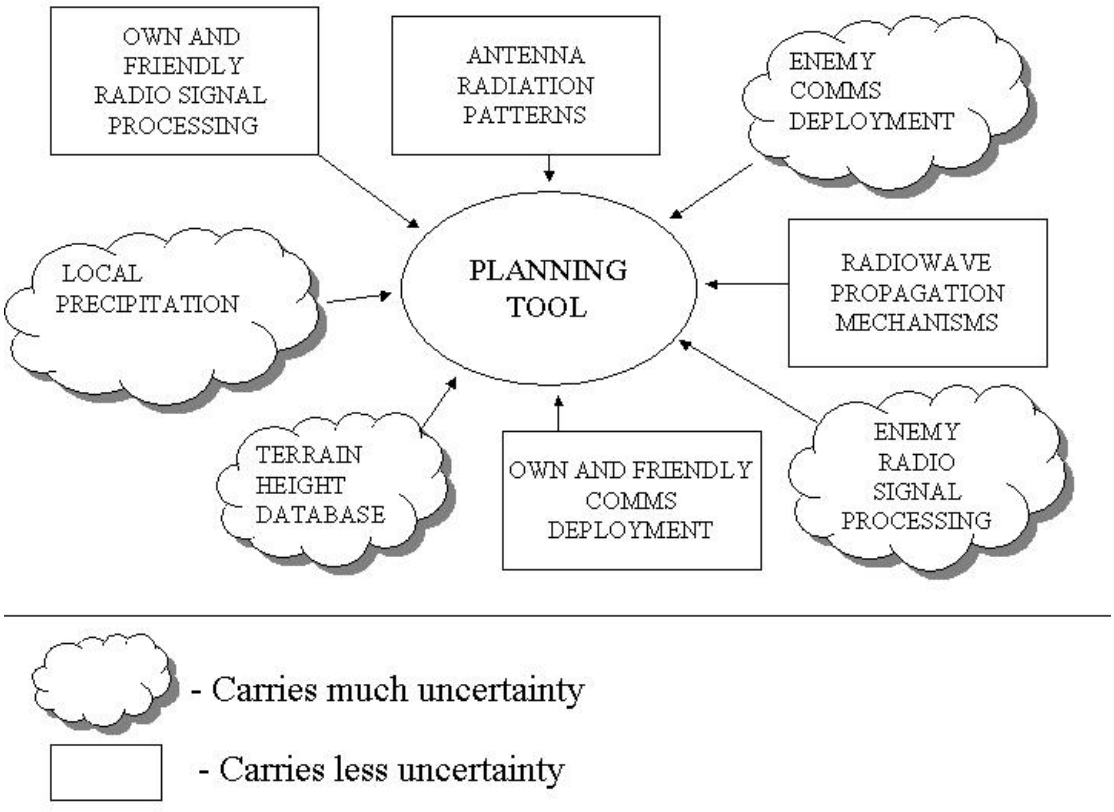

Figure 1 Important effects to be included in a communication planning tool

These estimates are frequency dependent, but may often give standard deviations of errors estimates in the order of 10 dB. This means that there is a huge difference between the median calculated signal and the signals obtainable for instance at 1 % or 99 % of the positions. The uncertainty is associated with position, and propagation will therefore not change much with time. This effect must therefore be taken into account in the planning tool, usually by adding or subtracting power margins according to what certainty you want to have associated with your actions.

Uncertainty of attenuation of radio waves in the 'precipitation limited' domain is mainly associated with the amount of rain that falls with a given intensity at a given percentage of the time at a particular site. This effect may or may not be included in a planning tool for tactical communications. The effect could be included in order to estimate if rainfall may be a reason for sudden dropout of a communication link. The heavy rainfall effect is usually local in nature, and should therefore not be included when dimensioning the power budget of a network that allows alternative routing.

2.2 Uncertainty related to enemy communication structure and jamming capability

The second communications planning system building block which is involving high uncertainty is the deployment of enemy communication structure. Using own communication Electronic Support Measures (CESM) to detect, identify and position the enemy gives only part of the data needed to plan against his use of the frequency spectrum. It is for instance more difficult to reveal his emitter power or antenna gains and direction. Nevertheless, these parameters may partly be deduced from analysis, and partly guessed from his modus operandi. The uncertainties after ESM analysis, associated with enemy deployment of communications equipment, may be of the order of 10 dB, very dependent on the frequency and the gain of the antennas. This is of the same order as the uncertainty associated with propagation modeling. There is no easy way to estimate the distribution of these errors, but one might get a rough estimate by identifying frequencies and systems that are involved.

Evaluating the effect of own radio systems subjected to hostile jamming has many parallels to the interference considerations performed for planning of conventional radio communication systems. The radio propagation mechanisms involved are fairly well understood and can be modeled with reasonable accuracy when input parameters like terrain profile, weather conditions, deployment structure antenna height and radiation diagrams are known. In a conventional communication scenario these parameters are static (except for the weather that is usually described statistically), but in a tactical, military setting the deployment of own and enemy forces will be non-static. Moreover, the power level and the waveform used by the enemy jamming equipment are not known in advance. Evaluation of own communication systems' vulnerability to hostile jamming waveforms may to some extent be considered a more accurate task, as the system receiver characteristics are normally well known and understood. Also, the testing and evaluation process can be performed under controlled environments. Nevertheless, in the calculations one must make some kind of 'educated guess' of the enemy's jamming capabilities. We suggest that the following three situations are analyzed:

The enemy jammer is transmitting band-limited white gaussian noise
The enemy jammer is transmitting CW (sweep or pulse)
The enemy jammer is transmitting worst-case signal matched jamming waveform[1]

Estimates of the output level for the enemy jammer can be based on previous experiences/intelligence. The 'timing' of jamming (in which situations jamming is used) must be based on empirical experiences (modus operandi).

As such analyses are based on several assumptions, the result will carry a considerable amount of uncertainty. The results may nevertheless indicate best- case or worst- case outcomes.

2.3 Uncertainty related to friendly jamming capability

Evaluating (predicting) the effect of own jamming involves most of the same entities as the hostile jamming situation. However, this situation is very different when it comes to which parameters we know exactly and which parameters that have to be estimated with uncertainty.

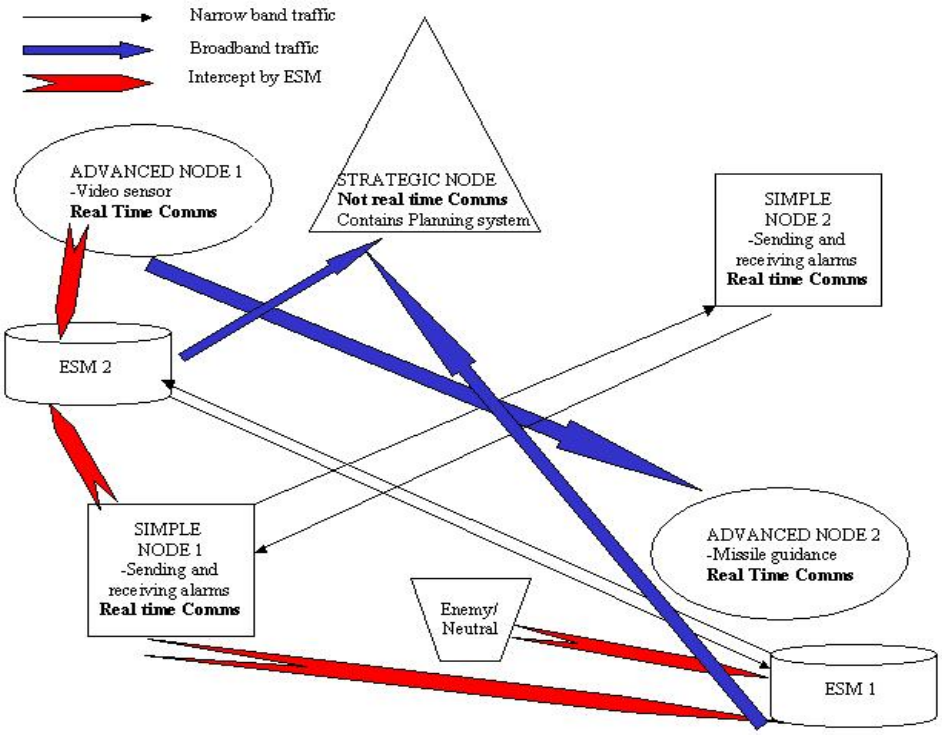

Figure 2 Illustration of information flows in an integrated EW-NCW concept, in a setting where the main task of ESM is monitoring own communications

Again we do not have the opportunity to test our predictions. First of all we do not normally have access to enemy equipment, furthermore one is normally very reluctant to test offensive EW systems 'live' as this might reveal our capacity. For the purpose of predicting the effect of

[1] The worst-case signal matched jamming waveform will be estimated as part of the evaluation of own system vulnerability.

own jamming one assumption that can be made is to relate the counterpart systems robustness against jamming to our own systems robustness (for instance half/equally/twice as robust). Naturally this may not be a very good estimate, but it may nevertheless be the best one can do in a situation where exact data are not available.

2.4 Complicating factors: alternative routing and 'graceful degradation'

One of the strengths of network centric military radio communications is obvious; the ability to reroute information if necessary. This effect, which will reduce the severity of consequences, will have to be taken into account when using a planning tool for calculating consequences with their associated probabilities. Thus calculating the probability of interference of single links alone is of little use. For each situation one has to consider the joint probability of retaining the necessary bandwidth capability over alternative routes between information providers and end-users. This may become a quite complicated task, particularly if 'necessary bandwidth' becomes negotiable. New communication applications, applied in military network centric settings, are likely to tolerate such 'graceful degradation', which means that reduced bandwidth results in reduced functionality. This means that the terms 'interference' and 'jamming' we have discussed so far in this paper are not any longer absolute, but become graded. In this setting a communication path may become 'somewhat' interfered with or 'somewhat' jammed.

3 CONCLUSION AND FURTHER WORK

In this paper we have outlined some key considerations for protecting the radio side of Network Centric Warfare, and we have suggested a communications planning system and methods to quantify the relevant uncertainties involved.

The complete communication planning system will also have uncertainties associated with other factors, such as missing information, for instance about own or neutral deployment of communications emitters. The success of the planning tool depends heavily on the deployment and integration of communications ESM equipment as part of the ordinary communications network. As well as surveillance of enemy actions, ESM should be used to monitor own activity, to make sure that resources are spent the way they were planned to. It is a fact of life that in tactical communications an operator often changes position or frequency or both in order to achieve success. Interference problems are therefore common in advanced communication scenarios. Potential interference problems can be discovered and dealt with if enemy, neutral and own communications are monitored constantly and everywhere and analysed in the same database.

REFERENCES

(1) M. Hata, ”Empirical formula for propagation loss in land mobile radio services”, IEEE Trans. Veh. Technol., vol. VT-29, NO. 3, Aug. 1980