FOI-R--1405--SE
December 2004
ISSN 1650-1942
**User report**

Sara Linder, Peter Stenumgaard, Ulf Sterner, Peter Svenmarck

# Intersystem Interference Risks in the Future Swedish Defence


Command and Control Systems
SE-581 11 Linköping

SWEDISH DEFENCE RESEARCH AGENCY

Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping

FOI-R--1405--SE

December 2004

ISSN 1650-1942

**User report**

Sara Linder, Peter Stenumgaard, Ulf Sterner, Peter Svenmarck

# Intersystem Interference Risks in the Future Swedish Defence

**Issuing organization**
FOI – Swedish Defence Research Agency
Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping

**Report number, ISRN**
FOI-R--1405--SE

**Report type**
User report

**Research area code**
4 C4ISTAR

**Month year**
December 2004

**Project no.**
E7956

**Sub area code**
41 C4I

**Sub area code 2**

**Author/s (editor/s)**
Sara Linder
Peter Stenumgaard
Ulf Sterner
Peter Svenmarck

**Project manager**
Sara Linder

**Approved by**
Martin Rantzer

**Sponsoring agency**
FMV

**Scientifically and technically responsible**
Peter Stenumgaard

**Report title**
Intersystem Interference Risks in the Future Swedish Defence

**Abstract (not more than 200 words)**
Efficient wireless communication is a prerequisite for realizing the idea of a Network Based Defence. For wireless communications, the issues of robustness and security are particularly important. The influence from intersystem interference is non-negligible. Hence, it is of significant importance to be able to estimate the risks for, and consequences of, intersystem interference at an early stage in the system design process.
Since the effects not only are dependent on the technical solutions, we have chosen to perform the analysis based on a number of scenarios and thus getting a broader view of the consequences. A communication network for a mechanized battalion has been simulated in a normal eletromagnetical environment and compared to a situation with intersystem interference. The consequences for the command and control of the battalion have been analysed. The risks of intersystem interference at an international operation have been investigated. Moreover, some emerging wireless technologies have been analysed with respect to intersystem interference.
The conclusion is that the existing methods for analysis of intersystem interference are not sufficient, since the effects on services and on human operators, for instance his/her trust, must be included. Furthermore, new methods are required to be able to evaluate the effects of intersystem interference on future flexible and dynamic communication systems built on software technology and ad hoc networks.

**Keywords**
intersystem interference, trust, ad hoc networks, intersystem interference tools, situation awareness

**Further bibliographic information**

**Language** English

**ISSN** 1650-1942

**Pages** 66 p.

**Price acc. to pricelist**

| Utgivare | Rapportnummer, ISRN | Klassificering |
|---|---|---|
| Totalförsvarets Forskningsinstitut - FOI | FOI-R--1405--SE | Användarrapport |
| Ledningssystem | **Forskningsområde** | |
| Box 1165 | 4. Ledning, informationsteknik och sensorer | |
| 581 11 Linköping | **Månad, år** | **Projektnummer** |
| | December 2004 | E7956 |
| | **Delområde** | |
| | 41 Ledning med samband, telekom och IT- system | |
| | **Delområde 2** | |



| Författare/redaktör | Projektledare |
|---|---|
| Sara Linder | Sara Linder |
| Peter Stenumgaard | **Godkänd av** |
| Ulf Sterner | Martin Rantzer |
| Peter Svenmarck | **Uppdragsgivare/kundbeteckning** |
| | FMV |
| | **Tekniskt och/eller vetenskapligt ansvarig** |
| | Peter Stenumgaard |


**Rapportens titel (i översättning)**

Telekonfliktrisker i det framtida försvaret


**Sammanfattning (högst 200 ord)**

Effektiva trådlösa kommunikationslösningar är en förutsättning för att kunna realisera idén med det nya nätverksbaserade försvaret. Dessa är dock särskilt känsliga när det gäller robusthet och säkerhet. En icke försumbar påverkan kommer från egengenererad störning (telekonflikt). Det är betydelsefullt att redan på systemutformningsstadiet kunna bedöma riskerna för och konsekvenserna av telekonflikt.

Eftersom effekterna inte bara beror av tekniska lösningar, har vi valt att genomföra studien baserat på scenarion och därmed få en mer heltäckande konsekvensbild. Påverkan på kommunikationsnätet för en mekaniserad bataljon har simulerats i en normal störningsmiljö och jämförts med en telekonfliktsituation. Konsekvenserna för ledning av bataljonen har sedan analyserats. Riskerna för telekonflikter vid en internationell insats har undersökts. Dessutom har några trender för framtida trådlösa kommunikationssystem analyserats med avseende på telekonflikt.

Slutsatsen är att dagens analysmetoder inte är tillräckliga, eftersom hänsyn också måste tas till påverkan på olika tjänster och på operatören, t.ex. dennes systemtilltro. Vidare behövs nya metoder, för att kunna bedöma hur framtida flexibla och dynamiska sambandssystem, som bygger på mjukvaruteknik och ad hoc nätteknik, påverkas.



**Nyckelord**

Telekonflikt, tilltro, ad hoc nät, telekonfliktverktyg, lägesuppfattning

| Övriga bibliografiska uppgifter | **Språk** Engelska |
|---|---|
| **ISSN** 1650-1942 | **Antal sidor:** 66 s. |
| **Distribution enligt missiv** | **Pris: Enligt prislista** |

# TABLE OF CONTENTS

# 1 INTRODUCTION

In Sweden there is an on-going development of the Armed Forces where the goal is the ability to execute operations more quickly and flexibly than today. For a long time, the Armed Forces were a large organisation. However, for a defence that is to be effective today and in the future, what counts is not so much quantity as the ability to execute operations quickly and flexibly.

The way chosen for the development of the Swedish Armed Forces is according to the concept of Network Based Defence. The idea of Network Based Defence is that with greater flexibility than before it will be possible to link together different military functions, such as information systems, decision-making and weapon systems, in a single networked organisation. In order to achieve the Network Based Defence concept, the requirements on the communication networks have substantially increased. For instance, the distribution of situation awareness data, which is likely to be a prioritised service, will lead to an increased data flow within the command and control system. A high capacity tactical mobile radio network, with ad hoc functionality, capable of conveying mixed services and applications, and the ability to support varying stringent quality-of-service demands, is an essential enabler for the NBD concept.

In the future many operations will be joint, with different combat arms working together and/or combined, with different nations involved. In addition the communications with civilian authorities and humanitarian organisations are also important. The need for reliable communications with parties outside the own organization is great.

In order to have reliable communications it is important to be able to analyse effects of intersystem interference. Known factors that increase the risk of intersystem interference are for example; more electronic systems on a platform, unpredictable co-location situations, combined and joint operations. In the future Armed Forces many of these risk factors can be found. Hence, the problem of intersystem interference is now more important to handle than ever.

The traditional approach to analyse intersystem interference is to investigate a static scenario with a fixed number of systems and with all parameters for these systems known. This approach is not possible in the future since the number of systems involved is rapidly growing and situations are not as predictable as they used to be. In addition to this the communication systems themselves are also going to be more dynamic and flexible, with parameters that might not be fixed.

The consequences from intersystem interference also have to be analysed differently. With a growing number of different services for a user and with different services, having different demands on the communication system, the analysis is more complex. The performance of an individual

communication link might not affect the end user in an ad hoc network; on the other hand it might affect the performance of other parts of the network.

## 1.1 Scope

This report summarizes the work performed by order FMV 270200-LB638249, 2003-10-29, which has been issued by Leif Junholm at the Swedish Defence Materiel Administration, Center of Expertise in Sensors & Telecommunications.

The purpose of the project was to identify and define sources of intersystem interference risks in order to support the work of verification and validation in development of command and control systems. In order to do this at least one relevant scenario should be analysed. Potential risks of intersystem interference in the scenario should be identified and consequences should be judged. The consequences should be analysed both at a system level and a system of systems level. The effects for an operator should be treated and also how this affects his confidence in the system. An investigation if other actors have ongoing activities about intersystem interference and Network Centric Warfare (NCW) shall be done.

## 1.2 Outline

In Chapter 2 a scenario of an international operation is described and intersystem interference risks in the scenario are investigated. In the future defence, situation awareness is assumed to be a prioritised service, and in Chapter 3 the service is evaluated in an ad hoc network with intersystem interference. The effects on operators' trust in services from intersystem interference are treated in Chapter 4. The intersystem interference risks with emerging technologies are described in Chapter 5. In Chapter 6 there is a ranking of future intersystem interference risks. The capabilities of present intersystem interference analysis methods are treated in Chapter 7 and the necessary capabilities of future intersystem interference tools are described in Chapter 8. Conclusions are given in Chapter 9. Finally some suggested topics for future work can be found in Chapter 10.

# 2 INTERSYSTEM INTERFERENCE RISKS IN A COMBINED OPERATION

In this chapter we discuss the risks of intersystem interference in combined operations. First we give a general description of intersystem interference risks in operations and give some specific examples of problems. Thereafter, a scenario with a peace-enforcement NATO mission is described and finally we discuss various parts of the scenario where there is a risk of intersystem interference.

## 2.1 General

Experience shows that most intersystem-interference problems typically occur in joint and combined operations; both at national and international level. This is often due to that precautions against interference problems are normally limited to single platforms or within single types of armed forces (i.e. sea, air and ground). When platforms and forces are mixed in joint operations, transmitting and receiving systems can start to interfere with each other in an unpredicted manner. Examples are [1]

- army or air force systems used on aircraft carriers.
- navy ordnance used in air force launchers.
- air-carried jammer and artillery counter-battery radar.
- a jammer aircraft experienced an engine shutdown when it began to transmit jamming signals.
- one of the radars of the aircraft carrier *USS Forrestal* ignited a rocket on one of the aircraft waiting to be catapulted (during the Vietnam war).
- The radar of the carrier *USS Eisenhower* had to be shutdown during Operation Uphold Democracy (Haiti 1994) not to ignite the Army helicopter *Black Hawk* ordnance.

Since future missions for the defence will be characterized by different kinds of joint and/or combined missions, this will increase the risk of new intersystem interference problems that have not been foreseen in the system development processes. At a national level there is also probable that civilian and military units will cooperate in a more close manner than before which will result in new intersystem-interference problems between the transmitting and receiving systems of these units. To be able to join international operations at sea, new equipment for interoperability with international rescue organizations must be installed on the Swedish navy vessels. Examples are wireless systems for communication and identification. This increases the risk of on-board intersystem interference problems on the vessels.

Spectrum management is a time-consuming activity in the initial phase of every international military operation. In operations of a larger scale such as in Kosovo and Iraq this process typically takes about two or three months. An important component of spectrum management is the

frequency assignment process, which gives the user (warfighter) the authority to operate a fielded, spectrum-dependent system. To prevent intersystem interference, coordination among all spectrum users within a frequency band and geographic region must occur. The regional frequency manager provides this coordination. For United Nation operations, frequency management for the forces is handled by the Joint Frequency Management Office of the Commander in Chief or Joint Task Force, working in conjunction with the host nation frequency management authorities. The seriousness of a military conflict does not necessarily permit the UN military forces unrestricted use of the spectrum. Local region commerce, public safety, and public service operations are expected to continue, to the extent possible, even in a conflict. This is especially true if the conflict is of limited intensity (e.g., peacekeeping operations), or of limited geographic scope (i.e., the conflict is in a small nation surrounded by border nations that are not involved in the conflict but are affected by electromagnetic transmissions in the conflict area). The ease with which UN forces can gain the necessary authorization from regional governments will generally depend on the extent to which commerce will be disrupted or whether anyone's national sovereignty is actually threatened. The effectiveness and the safety of the warfighter will be adversely affected if these effects are not understood. An already well-known problem is the lack of available frequencies for army combat frequency-hopping radios. The Swedish army combat radio Ra180/480 operates the frequency band 30-88 MHz. During international combined operations only one or a very few frequencies are allowed to be used. The reason for this restriction is to prevent intersystem-interference problems with radio systems from other countries in the same operation. This restriction severely degrades the robustness of the army combat radio since the frequency-hopping function is the fundamental function to enhance robustness against different kinds of interference.

An investigation if other actors have ongoing activities about intersystem interference and network centric warfare has been done. No such activity has been found. It was expected that such activity would be on going within the US Joint Spectrum Center (JSC) or SPAWAR systems center (San Diego) but no information of such activity has been found.

## 2.2 Scenario

At the Swedish National Defence College (SNDC) there has been a project about joint combat. The focus has been on command at an operative and tactical level in a network based flexible defence. A part of this work has been to analyse a scenario for a combined endeavour. The scenario is developed from a scenario used in the air force and navy's staff duty training at SNDC [2]. We have investigated intersystem interference risks in this scenario, but first a brief description of the scenario.

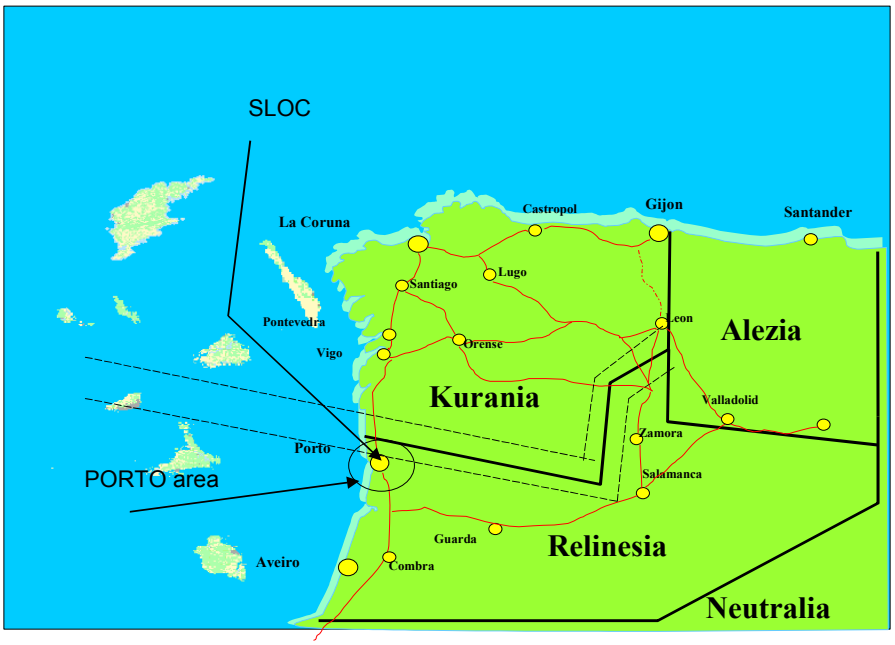


*Figure 2.1: The area where the scenario takes place.*

The fictitious countries, in which the scenario takes place, are Kurania, Relinesien, Alezia and Neutralia, see Figure 2.1. The countries are located on the Iberian Peninsula, i.e. in the real world parts of Portugal and Spain. There are also additional islands in the sea to the west of the peninsula.

The goal of the operation is to re-establish the regional stability. Criteria for this include that Relinesien and Kuranien remain with their cease-fire agreement and that the belligerents respect international human law.

In this scenario, at D-day the joint force headquarter (JFHQ) in Porto was surrounded by a mob of angry Relinesiens at the same time as the authorities in Relinesien turned off the water and electricity for the HQ. Prior to this development, the transports to and from the harbour have been obstructed several times. At this time, Relinesien mined the navigable channel to the harbour and blocked the airfield north of Porto. Shortly afterwards the Relinesian government demanded that UN and NATO should leave Relinasian and Kuranian territory.

The commanding officer (CO) of the first multinational division (1. MND), of which the Nordic brigade is a part, is in charge of liberating the HQ in Porto. The 1. MND together with the 2. MND and supporting troops constitute the land component command (LCC). LCC is supported by the marine component command (MCC) and air component command (ACC). The CO of 1. MND must be ready to evacuate the HQ staff. The 1.MND CO leads the liberation operation from a Visby corvette.

Relinesien have grouped a battery of surface-to-air missiles of type SA-10 at the airfield. The Relinesian troops have surrounded the JFHQ with approximately a battalion. Another battalion is probably located at the airfield and two or three battalions are positioned in the city centre and at the harbour.

At night D+6 days, the operation to liberate the HQ is started. An amphibious battalion and an airborne battalion support the Nordic brigade. Two mechanized battalions from the Nordic brigade advance from the east. At the same time as the mechanized battalions reach the city centre the amphibious battalion is planned to land north of the old fishing harbour in order to quickly rescue the staff at the headquarter. The mission of the airborne battalions is to reinforce the defence of the HQ. The airborne battalion is planned to land in the park west of the HQ after it is secured.

The clearance of mines in the channel is started after the amphibious battalion has landed in order not to reveal the landing. Two Visby corvettes support the landing. The opponent's marine forces are blocked in their bases. Also, the maritime forces are responsible for communications intelligence and electronic warfare. In addition, the maritime forces carry out anti-submarine warfare.

Air assets attack bridges in the east in order to guard the flank of the advancing brigade. The air assets are also responsible for reconnaissance in the east and south. When the brigade starts its attack it should be protected by close air support and the ships/navy should also be protected. Also, the enemy's air bases and operating bases shall be attacked. The enemy's SA-10 shall at this time be engaged, either by suppression of enemy air defences (SEAD) or destruction of enemy air defence (DEAD).

## 2.3 Intersystem Interference Risks in the Scenario

There are three Swedish corvettes of Visby class in the first surface action group (1. SAG). In this group there are also ships from the United Kingdom, Germany, Canada, France, Belgium, Denmark and Greece. From an intersystem interference point of view, there are a number of different systems that use the same frequency band. All ships have at least one radar system and many of them are also capable of jamming radar systems. Hence, careful frequency planning is required. For example, Visby can carry out electronic signal monitoring (ESM) in the frequency band 2-18 GHz. In this frequency band several radar systems are operating. Great precaution should be taken so friendly radar, or worse jamming, does not illuminate the surveillance systems. On Visby there are some ideas about introducing a communication link to sonar buoys and in that case the communication would be in the Ku-band (12-18 GHz). In this frequency band, both radar and jamming systems operate. Since especially jamming often uses high power there is a high possibility of intersystem interference. In tables 2.1 and 2.2 a brief summary of intersystem interference risks is shown for Visby in the first surface action group.

| Type | Class | Nation | Visby ESM 2-18 GHz | Visby radar system 4-8 GHz | 12-18 GHz |
|---|---|---|---|---|---|
| CVGH | INVINCIBLE | UK | X | | |
| DDHM | CASSARD | FR | X | X | |
| FFA | WIELINGEN | BE | X | | |
| DDGH | TRIBAL | CA | X | | X |
| FFA | NIELS-JUEL | DA | X | X | X |
| FFAH | BRANDENBURG | GE | X | | |
| FFAH | SACHSEN | GE | X | | |
| FFAH | HYDRA | GR | X | X | |

*Table 2.1: Radar systems on other ships.*

| Type | Class | Nation | Visby ESM 2-18 GHz | Visby radar system 4-8 GHz | 12-18 GHz |
|---|---|---|---|---|---|
| CVGH | INVINCIBLE | UK | X | X | X |
| DDHM | CASSARD | FR | X | X | X |
| FFA | WIELINGEN | BE | | | |
| DDGH | TRIBAL | CA | | | |
| FFA | NIELS-JUEL | DA | X | X | X |
| FFAH | BRANDENBURG | GE | X | X | X |
| FFAH | SACHSEN | GE | X | X | X |
| FFAH | HYDRA | GR | X | X | X |

*Table 2.2: Radar jamming systems on other ships.*

The amphibious (AMPH) group consists of units from the Netherlands, the United Kingdom and Sweden. The AMPH group consist of six Landing Personnel Docks (LPD), three amphibious battalions, supporting troops and service support. The group operates tight together which increases the risk of intersystem interference between the systems onboard the ships. COTS electronics might also be used onboard the ships, which increases the risk of intersystem interference.

The mechanized battalions that are advancing through Porto might also experience intersystem interference. In Porto there are a number of civilian systems for communication, such as GSM, 3G, WLAN and radio services for public-safety agencies. The TV and radio networks in Porto are also functioning and might interfere with the wireless communication. In addition to this an increased noise level can be expected in a city due to man-made noise.

The airfield in Porto is protected by a battery of SA-10, which must be handled during the attack. The enemy's radar system works in the C- and X-band, or more precise between 7 and 11 GHz. The radar systems must

be jammed during the attack on the airfield, probably from airplanes. This takes place at the same time as there are a lot of other activities both on land and sea. Hence, the risk of intersystem interference or jamming of friendly forces is quite high.

In this scenario GPS systems are used for positioning. GPS uses two frequencies L1 and L2. Civilian GPS uses the frequency L1, 1575.42 MHz, while L2 (1227.60 MHz) is mainly for military use and controlled by US DoD. GPS is vulnerable for intersystem interference and jamming since the signal strength of the signals from the satellites are quite low at the receiver [3]. Military GPS can be designed against the threat of electronic attack and are therefore more robust against intersystem interference as well.

## 2.4 Conclusions

The analysis of the scenario shows several potential intersystem interference risks that should be more thoroughly analysed in a future activity. The analysis of the scenario confirms the well known experience that joint/combined operations creates intersystem interference risks that could be very difficult to identify in advance to an operation.

# 3 INTERSYSTEM INTERFERENCE RISKS AND AD HOC NETWORKS

## 3.1 Background

The ability to quickly acquire and assimilate information at all levels of the command hierarchy is fundamental in a network based defence. In many of the command and control systems projected, low level units are expected to make well informed and autonomous decisions. Combat information and sensor data must thus be available "on the move" even at the level of the individual soldiers.

In crucial situations, e.g. communication on the battlefield itself, there will be a need for high performance wireless communication without the support of a pre-deployed infrastructure. In these cases a radio network should be able to be successfully deployed in unknown terrain and with a minimum need of network planning. One method for obtaining area coverage in this type of networks is to enable radio units to relay messages, thus creating a so called *multi-hop* network. Furthermore, the networks should utilize distributed network control to increase robustness e.g. in the event of node annihilation. Such networks are often referred to as *ad hoc* networks. The network also has to remain intact as the units move rapidly into new terrain. Network protocols must therefore be able to cope with rapid and unexpected topology changes caused by the movements of the radio units.

It is also foreseen that the quantity of electronic equipments, such as computers, will increase at the battlefield. Since many of the electronic equipments radiate electromagnetic energy, intentionally or unintentionally, this will result in a higher risk of intersystem interference. The effects of intersystem interference for digital communication system have been studied in [4, 5]. Common for these reports is that they focus on the effects of intersystem interference, in terms of bit error rate, for one communication link.

However, the communication system in the future consist of many links forming a network which supports the users with different services [6, 7], e.g. group calls, situation awareness data, and intranet connections. It is therefore also important to be able to estimate the impact of the intersystem interference on a network, and the services the network supports.

In this study, we analyse how the performance of a Situation Awareness (SA) service is affected by intersystem interference in an ad hoc network. The evaluation is performed for a tactical scenario in form of a mechanised battalion that attacks a hostile air-landing.

## 3.2 Tactical Scenario

We consider a scenario for a Swedish mechanised battalion. This battalion is simplified to consist of one type of communication platform only, a vehicle. Furthermore, we assume that a battalion consists of 6 companies, four tank/APC companies with 24 vehicles each, one command and artillery company with 20 vehicles, and one pioneer (or support) company with 39 vehicles. Altogether, we have 155 vehicles, or communication nodes.

The scenario is set up as armed combat on Swedish ground. The tactical scenario was developed in the project "Communication for tactical command and control" and details about how the units are moving are described in [6].

In the scenario, the task for the mechanised battalion is to strike out a hostile air-landing within an assigned area, and be prepared to strike out air-landings in adjacent areas. An area around Skara was selected, where most parts of the terrain are rather flat and covered by meadows and groves. First, the battalion is spread out and grouped within the main anticipated drop zone. Thereafter, the anticipated airdrop is found out to take place in an adjacent area. This leads to a high-speed movement of the combat vehicles (speed of up to 20 m/s) on roads to the air-landing zone 10-20 km away.

### 3.2.1 Situation Awareness (SA) Service

It is becoming increasingly important to have information about other nodes in the network, such as their position, speed, and direction of movement, to avoid fratricide and to maintain information superiority. Hence, future communication systems are expected to support SA services [6].

The user requirement on the SA service we use is that the uncertainty in estimated positions should be less than 20 meter for all nodes closer than 3 km, less than 200 meter for all nodes between 3 and than 15 km and less than 500 m for all nodes between 15 and 30 km [6]. However, since few nodes are outside 15 km range, in the scenario that we use, we choose to use the 200 m requirement for all nodes beyond 3 km.

If we assume that the velocity of the nodes is 72 km/h or 20 m/s we can transform the demand to that the SA information for nodes closer than 3 km should not be older than 1 s and the information for nodes more than 3 km away should not be older than 10 s.

## 3.3 Radio Network Model

### 3.3.1 Link model

An essential part of modelling an on-ground or near-ground radio network is the electromagnetic propagation characteristics due to the terrain

variation. A common modelling approach is to use the basic path-loss, $L_b$, between two nodes (radio units). To estimate the basic path-loss between the nodes, we use an uniform geometrical theory of diffraction (UTD) model by Holm [8]. To model the terrain profile, we use a digital terrain database. All our calculations of the basic path-loss are carried out using the wave propagation library DetVag-90® [9].

For any two nodes $(v_i,v_j)$, where $v_i$ is the transmitting node and $v_j \neq v_i$, we define the signal-to-noise ratio (SNR), $\Gamma_{ij}$, here defined as $E_b/N_0$, in the receiving node $v_j$, as

$$\Gamma_{ij} = \frac{PG_T(i,j)G_R(i,j)}{N_R L_b(i,j)R_{ij}},$$

where $P$ denotes the power of the transmitting node $v_i$ (equal for all nodes), $G_T(i,j)$ the antenna gain of node $v_i$ in the direction of node $v_j$, $G_R(i,j)$ the antenna gain of $v_j$ in the direction of $v_i$, $N_R=FkT_0$, the noise in the receiver, where $F$ is the receiver noise factor, $k$ is Boltzmans constant, $T_0$=290 K, $R$ is the data rate, and $L_b(i,j)$ is the basic path-loss between nodes $v_i$ and $v_j$.

We assume that a packet from node $v_i$ can be received in node $v_j$ if SNR is not less than a threshold $\gamma_0$, i.e.

$$\Gamma_{ij} \geq \gamma_0.$$

The values of the parameters that are fixed during our simulations are set according to Table 3.1.

| P | $G_T(i,j)$ | $G_R(i,j)$ | $kT_0$ | $\gamma_0$ |
|---|---|---|---|---|
| 50 W | 1 | 1 | $4 \times 10^{-21}$ W/Hz | 15 dB |

*Table 3.1: Parameters used in the simulations.*

### 3.3.2 Reduced models for intersystem interference

To predict the consequences on higher system level in the network, reductions in the intersystem-interference modelling have been done on the platform (node) level. These reductions are summarized as follows.

- The only information that has been used about the radiated interference-signals is the signal power.
- Only signals within the receiver bandwidth have been considered.
- The antenna directivity of the interfering equipment has been assumed to be 0 dB in all directions.

- The shielding effectiveness of the platform fuselage has been reduced to a fixed number for all frequencies of interest. This number has been chosen with knowledge about typical values of shielding effectiveness from measurements on combat vehicles.

The wave-propagation modelling between radiated interference source and radio communication antenna has been reduced to only be dependent on the separation distance between the interfering device and receiving antenna. The model for the dependence of separation distance has been selected from [38].

### 3.3.3 Data Link Layer

In this study, we use a Time Division Multiple Access (TDMA) based Multiple Access Control protocol, see [10]. TDMA is a static collision-free, protocol where the channel sharing is done in the time domain. We here choose to use a node-oriented TDMA protocol where the time is divided into time slots, with duration $T_s$, and each node is assigned one or several time slots where it is allowed to use the channel. An alternative, which is less suitable for broadcast traffic but might work better when spatial reuse is considered, is a link-oriented protocol [11].

Since this study is focused on the performance of the SA service and not on the performance of the MAC protocol, we use at rather optimal method to decide which node may use a certain slot. According to this method, we determine at each time slot, which node that has the oldest queued packet. This node is then allowed to use the time slot. For simplicity, the slot assignment in our simulation is centralised, there are, however, ways to distribute the slot assignment, see [12].

### 3.3.4 Fisheye State Routing

To find suitable routes in the network we use the Fisheye State Routing (FSR) protocol. FSR is a proactive link state protocol whose objective is to keep control traffic low and still provide accurate information about the routes, see [13]. The FSR protocol uses the Fisheye technique, which was originally used to reduce data required to represent graphical data. According to this technique, a node's perception of its surroundings, is similar to that of a fisheye, where the level of detail is high near the “focal point” and decreases with the distance from the focal point. This means that when a user packet is sent, the intermediate nodes will have increasingly better routing information available as the packet approaches its destination and will use this to gradually improve the route.

### 3.3.5 Distributing SA Information Using Routing Update Messages

When using a proactive routing protocol, such as Fisheye State Routing (FSR), the nodes continuously try to uphold routes to one another. This means that periodically there will be routing control traffic flowing through the network, see [14]. An efficient method of distributing SA data might

thus be to “piggyback” the SA data onto existing control traffic. Since our current implementation of this SA algorithm is not optimised for the used demands on the SA service, we choose to ignore the amount of traffic the SA service generates and focus on how the connectivity of the network influence the availability of the SA service.

## 3.4 Simulation Results

In this section we present the results from the different simulations carried out on the used scenario. Two types of intersystem interference scenarios have been simulated, one where all nodes have intersystem interference, and one where only the command vehicles at battalion and company level have intersystem interference. The receiver noise factor has been simulated for $F$ = {10, 22, 33, 44} dB, where $F$=10 dB corresponds to no intersystem interference. The higher values of $F$ corresponds to having a computer fulfilling the emission level in EN55022 class B, at a distance of 20, 10, and 3 m. The calculations can be found in appendix A. The difference between the noise figures can also be explained as different shielding between the interference source and the antenna. The data rate on the links have been simulated for $R$ = {0.5, 1.0, 2.0} Mbit/s.

First, we present results concerning the connectivity of the network. We will then show estimates of the availability of the SA service and estimates of the error in the SA service. In all network plots, all the units in a platoon are represented by one dot.

### 3.4.1 Network Connectivity

In Figure 3.1 we present an example of the network connectivity for a network without intersystem interference and a data rate of 1.0 Mbit/s. As we can se the network is fully connected when there is no intersystem interference. In Figure 3.2 we present an example of the network connectivity for a scenario where all nodes have intersystem interference, F = 33 dB, and a data rate of 1.0 Mbit/s.

If we compare Figure 3.1 and 3.2 we can se that the network connectivity decreases substantially when intersystem interference is introduced. However, inside the platoons the connectivity is still high since the communication distance is rather short, so the service availability for nodes closer than 3 km is still over 50%, even if the network seems to have fallen totally apart in Figure 3.2.

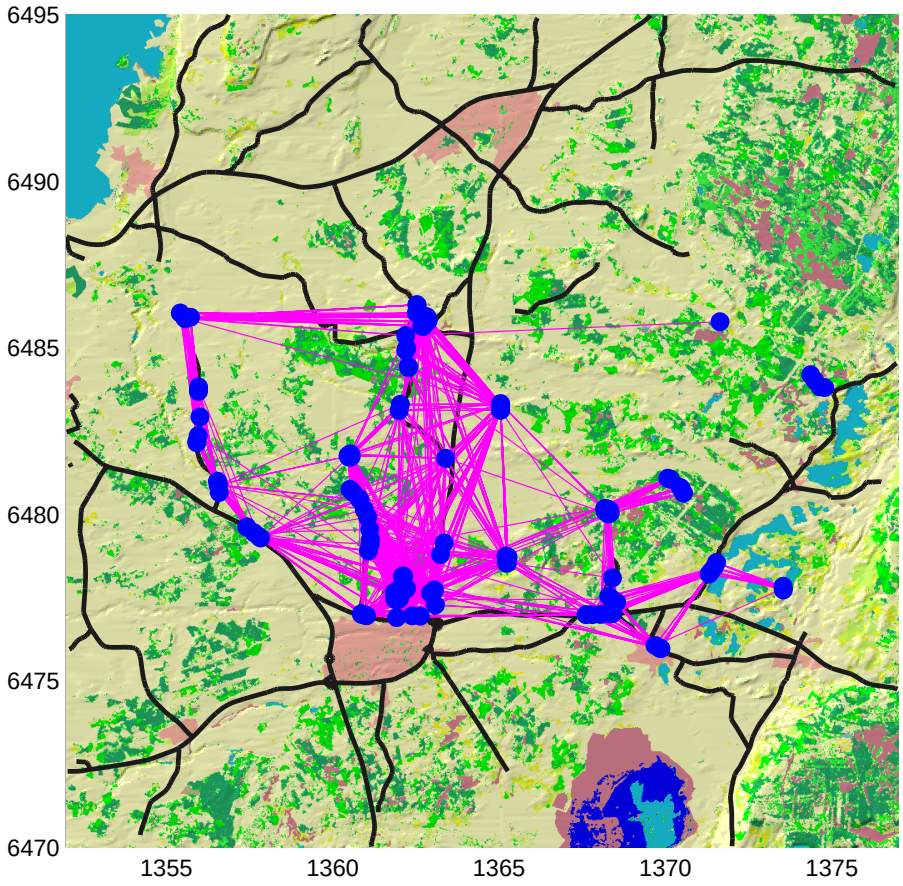


*Figure 3.1: Connectivity of the network with no intersystem interference, i.e.* F*=10 dB, and a data rate of 1.0 Mbit/s.*

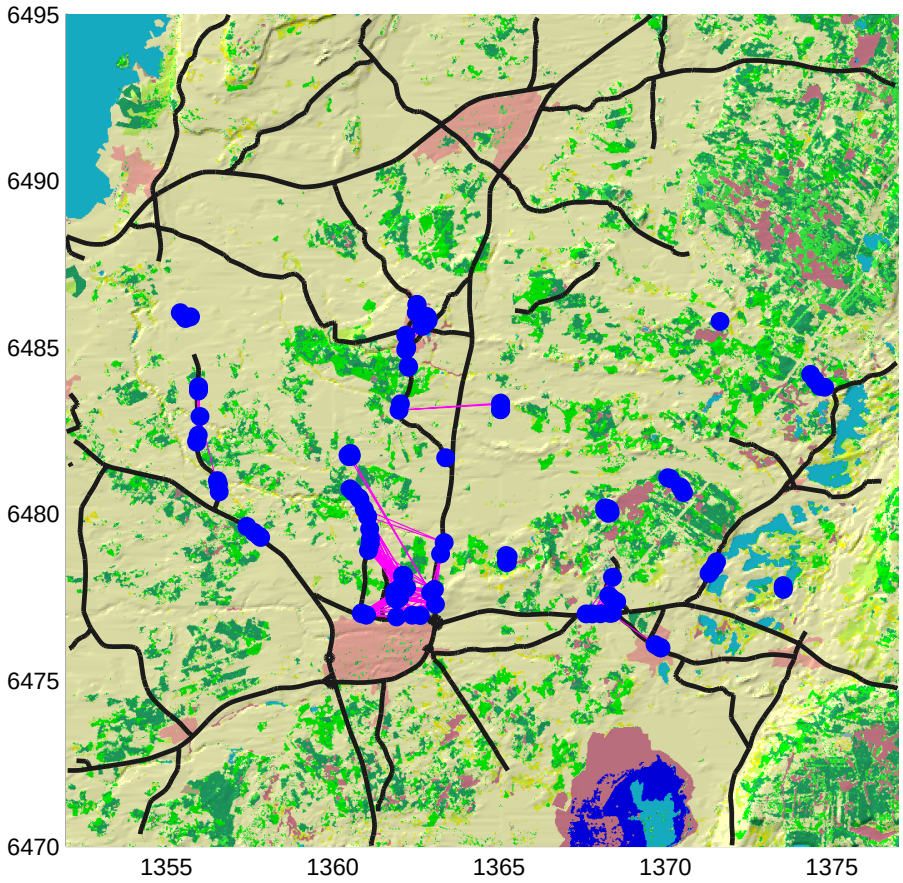


*Figure 3.2: Connectivity of the network when all nodes have an intersystem interference corresponding to a computer at a distance of 10 m, i.e. F = 33 dB, and a data rate of 1.0 Mbit/s.*

### 3.4.2 SA service availability

The mean service availability is presented in Table 3.2-3.4 for different data rates, {0.5, 1.0, 2.0} Mbit/s. The mean service availability is presented for all nodes in the network and for the command vehicles. The results are shown for nodes within or beyond 3 km of each other.

In Table 3.2 we can see that the service availability is 1.0 when there is no intersystem interference. We can also see that the service availability for a scenario where all nodes have intersystem interference decreases when the intersystem interference increases, especially the availability for nodes that are more than 3 km away. However, the service availability for scenario where only the command vehicles have intersystem interfere is hardly affected at all when we increase the intersystem interference, even when we consider the service availability for the command vehicles. From this we can conclude that even if a node loses links due to intersystem interference the nodes service availability can be unaffected as long as the node is connected to the network by other links. However, it is likely that the total network capacity is affected in a negative way by the intersystem

interference. So if we where also considering the network capacity the SA service might be affected in a negative way by the intersystem interference.

| Nodes with interference | $F$ | Service availability for all nodes $d < 3$ km | Service availability for all nodes $d > 3$ km | Service availability for command vehicles $d < 3$ km | Service availability for command vehicles $d > 3$ km |
|---|---|---|---|---|---|
| None | 10 dB | 1.0 | 1.0 | 1.0 | 1.0 |
| All | 22 dB | 0.99 | 0.95 | 0.99 | 0.93 |
| | 33 dB | 0.91 | 0.44 | 0.90 | 0.44 |
| | 44 dB | 0.66 | 0.04 | 0.62 | 0.05 |
| Command vehicles | 22 dB | 1.0 | 1.0 | 1.0 | 1.0 |
| | 33 dB | 1.0 | 1.0 | 1.0 | 1.0 |
| | 44 dB | 1.0 | 1.0 | 0.96 | 0.97 |

*Table 3.2: Service availability for different interference levels for a data rate of 0.5 Mbit/s. The availability is either averaged over all nodes inside/outside 3 km or averaged only over the command vehicles inside/outside 3 km.*

| Nodes with interference | $F$ | Service availability for all nodes $d < 3$ km | Service availability for all nodes $d > 3$km | Service availability for command vehicles $d < 3$ km | Service availability for command vehicles $d > 3$ km |
|---|---|---|---|---|---|
| None | 10 dB | 1.0 | 1.0 | 1.0 | 1.0 |
| All | 22 dB | 0.98 | 0.86 | 0.98 | 0.84 |
| | 33 dB | 0.86 | 0.30 | 0.84 | 0.29 |
| | 44 dB | 0.61 | 0.02 | 0.55 | 0.03 |
| Command vehicles | 22 dB | 1.0 | 1.0 | 1.0 | 1.0 |
| | 33 dB | 1.0 | 1.0 | 0.99 | 1.0 |
| | 44 dB | 1.0 | 1.0 | 0.95 | 0.96 |

*Table 3.3: Service availability for different interference levels for a data rate of 1.0 Mbit/s. The availability is either averaged over all nodes inside/outside 3 km or averaged only over the command vehicles inside/outside 3 km.*

| Nodes with interference | $F$ | Service availability for all nodes $d < 3$ km | Service availability for all nodes $d > 3$km | Service availability for command vehicles $d < 3$ km | Service availability for command vehicles $d > 3$ km |
|---|---|---|---|---|---|
| None | 10 dB | 1.0 | 0.99 | 1.0 | 0.99 |
| All | 22 dB | 0.97 | 0.72 | 0.96 | 0.71 |
| | 33 dB | 0.78 | 0.13 | 0.75 | 0.15 |
| | 44 dB | 0.58 | 0.02 | 0.52 | 0.02 |
| Command vehicles | 22 dB | 1.0 | 0.99 | 1.0 | 0.99 |
| | 33 dB | 1.0 | 0.99 | 0.98 | 0.98 |
| | 44 dB | 0.99 | 0.99 | 0.94 | 0.94 |

*Table 3.4: Service availability for different interference levels for a data rate of 2.0 Mbit/s. The availability is either averaged over all nodes inside/outside 3 km or averaged only over the command vehicles inside/outside 3 km.*

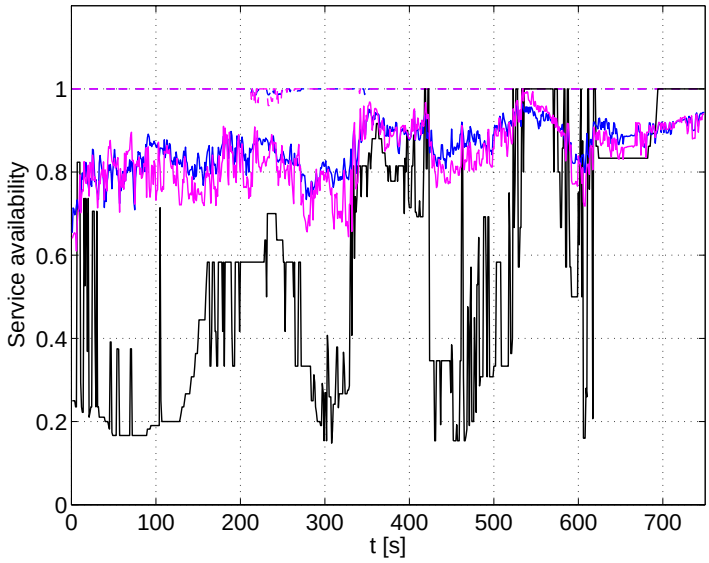


*Figure 3.3: Average service availability for nodes within 3 km. The dashed lines represent a network without intersystem interference, i.e. F=10 dB. The solid lines represent a network where all nodes have intersystem interference corresponding to a computer at a distance of 10 m F=33 dB. The {**blue**, **magenta** } lines represent the average service availability for {**all nodes**, **command vehicles**} in the battalion. The **black** line represents the average for the command vehicle with the lowest service availability.*

If we compare the results in Table 3.2-3.4 we can see that the service availability decreases with increasing data rate. This is due to the fact that the network connectivity decreases when we increase the data rate on the links. In Table 3.2-3.4 we can also see that there are no obvious difference between the service availability for the whole network and command vehicles when all nodes have intersystem interference.

To better understand how the service availability changes over time we have plotted the service availability as a function of time in Figure 3.3-3.4 for the scenario where all units have intersystem conflicts. Figure 3.3 shows the service availability for nodes that are closer than 3 km and Figure 3.4 shows the service availability for nodes more that are more than 3 km away.

In both figures the dashed lines represent a system without any intersystem interference and the solid lines represent a system with intersystem interference corresponding to a computer at a distance of 10 m, $F$=33 dB. Furthermore, the blue lines represents service availability for all nodes in the network, the magenta line represents the service availability for the command vehicles and the black line the service availability for the command vehicle with the lowest service availability.

In the figures we can see that even if the mean for the network and the command vehicles is relatively constant over time the mean for an

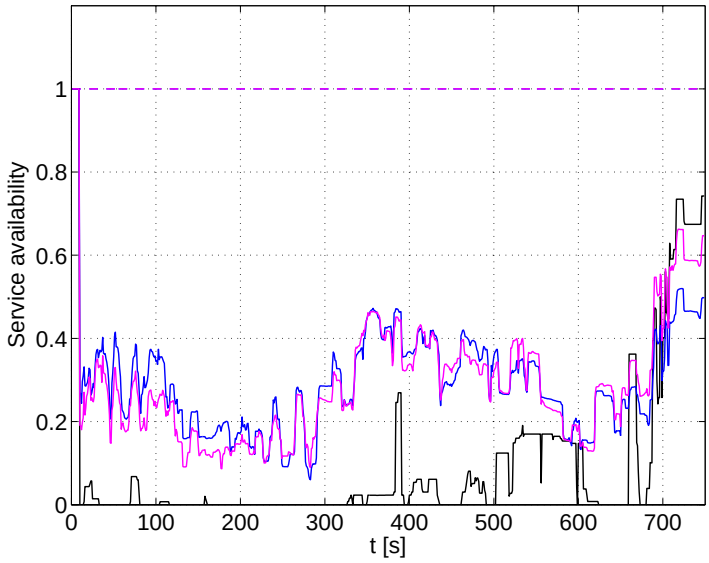


*Figure 3.4: Average service availability for nodes outside 3 km. The dashed lines represent a network without intersystem interference, i.e. F=10 dB. The solid lines represents a network where all nodes have intersystem interference corresponding to a computer at a distance of 10 m F=33 dB. The {**blue**, **magenta** } lines represent the average service availability for {**all nodes**, **command vehicles**} in the battalion. The **black** line represents the average for the command vehicle with the least service availability.*

individual node can vary considerably. If we compare Figure 3.3 and Figure 3.4 we can also se that the service availability is much lower for nodes that are more than 3 km away. An explanation for this can be found in Figure 3.1 where we can see that the network has fallen apart. The nodes will thus only have information about the nodes in their adjacent surroundings.

### 3.4.3 Position Error

To get an idea of the size of the position error when the service availability is less than 1.0, we also estimate the expected error for a node if the demands are not fulfilled. It is important to notice that if node $v_1$ does not get an update from node $v_2$ for 10 seconds we get a mean error of (10-1)/2=4.5 seconds if $v_2$ is in 3 km distance. A node with an error of 375 seconds thus corresponds to a node from which we do not get any position information from during the entire simulation.

In Table 3.5 we can se that the error increases when the intersystem interference increases. If we compare Table 3.5-3.7 we can also conclude that the error increases when the data rate increases. In both cases, the increase in errors is due to the lower network connectivity.

From Table 3.5-3.7 we can also se that there are no obvious difference between the error for the whole network and the error for the command vehicles.

| Nodes with interference | $F$ | Mean error for all nodes $d < 3$ km | Mean error for all nodes $d > 3$km | Mean error for command vehicles $d < 3$ km | Mean error for command vehicles $d > 3$ km |
|---|---|---|---|---|---|
| None | 10 dB | - | - | - | - |
| All | 22 dB | - | 41 | 5.7 | 34 |
| | 33 dB | 24 | 140 | 26 | 140 |
| | 44 dB | 120 | 340 | 110 | 320 |
| Command vehicles | 22 dB | - | - | - | - |
| | 33 dB | - | - | - | - |
| | 44 dB | - | - | 31 | 49 |

*Table 3.5: Mean error in seconds for the service when it fails for a data rate of 0.5 Mbit/s. The error is either averaged over all nodes inside/outside 3 km or averaged only over the command vehicles inside/outside 3 km.*

| Nodes with interference | $F$ | Mean error for all nodes $d < 3$ km | Mean error for all nodes $d > 3$km | Mean error for command vehicles $d < 3$ km | Mean error for command vehicles $d > 3$ km |
|---|---|---|---|---|---|
| None | 10 dB | - | - | - | - |
| All | 22 dB | 6.7 | 56 | 8.3 | 52 |
| | 33 dB | 43 | 190 | 42 | 200 |
| | 44 dB | 160 | 350 | 180 | 340 |
| Command vehicles | 22 dB | - | - | - | - |
| | 33 dB | - | - | 3.8 | - |
| | 44 dB | - | - | 46 | 69 |

*Table 3.6: Mean error in seconds for the service when it fails for a data rate of 1.0 Mbit/s. The error is either averaged over all nodes inside/outside 3 km or averaged only over the command vehicles inside/outside 3 km.*

| Nodes with interference | $F$ | Mean error for all nodes $d < 3$ km | Mean error for all nodes $d > 3$km | Mean error for command vehicles $d < 3$ km | Mean error for command vehicles $d > 3$ km |
|---|---|---|---|---|---|
| None | 10 dB | - | 31 | - | 22 |
| All | 22 dB | 17 | 82 | 18 | 82 |
| | 33 dB | 41 | 250 | 46 | 260 |
| | 44 dB | 190 | 360 | 220 | 350 |
| Command vehicles | 22 dB | - | 29 | 4.5 | 24 |
| | 33 dB | - | 55 | 6.1 | 21 |
| | 44 dB | 95 | 55 | 120 | 120 |

*Table 3.7: Mean error in seconds for the service when it fails for a data rate of 2.0 Mbit/s. The error is either averaged over all nodes inside/outside 3 km or averaged only over the command vehicles inside/outside 3 km.*

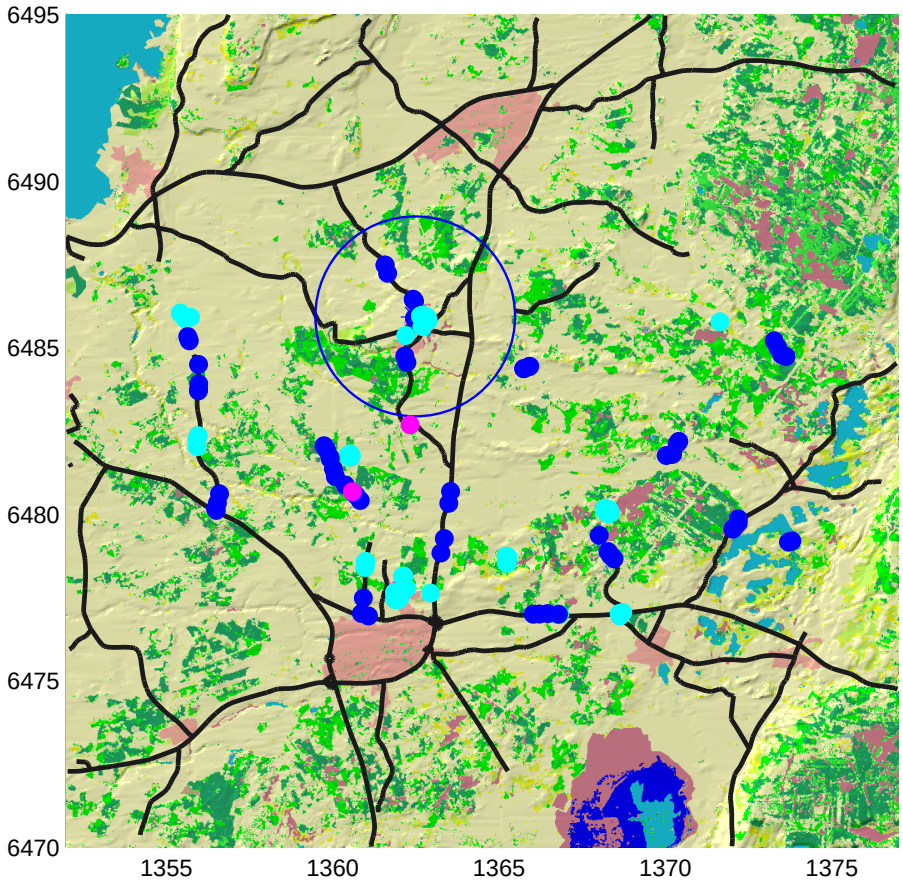


*Figure 3.5: Illustration of one nodes position information for the scenario with no intersystem interference. The node of interest is in the middle of the* ***circle*** *which represents the 3 km perspective of the node. The {****blue****,* ***cyan****,* ***magenta****} dots represents {****fighting vehicles****,* ***non fighting vehicles****,* ***command vehicles at battalion level****}.*

To further illustrate the availability of the SA service we can consider Figure 3.5-3.6. In these figures we have plotted the estimated positions for all vehicles from the node in the middle of the circle. The estimated position are plotted with dots.

If the position fulfils our demands the position is represented by a blue dot if it is a fighting vehicle, a cyan dot if it represent non-fighting vehicle, and a magenta dot if it represent a command vehicles at battalion level.

However, if a node's position does not fulfil our demands the node is marked with a lighter version of the colour. Furthermore, the node's real position is marked with a trail that begins at the estimated position and ends up at the real poison. The size of the trail can thus be seen as an estimate of the position error.

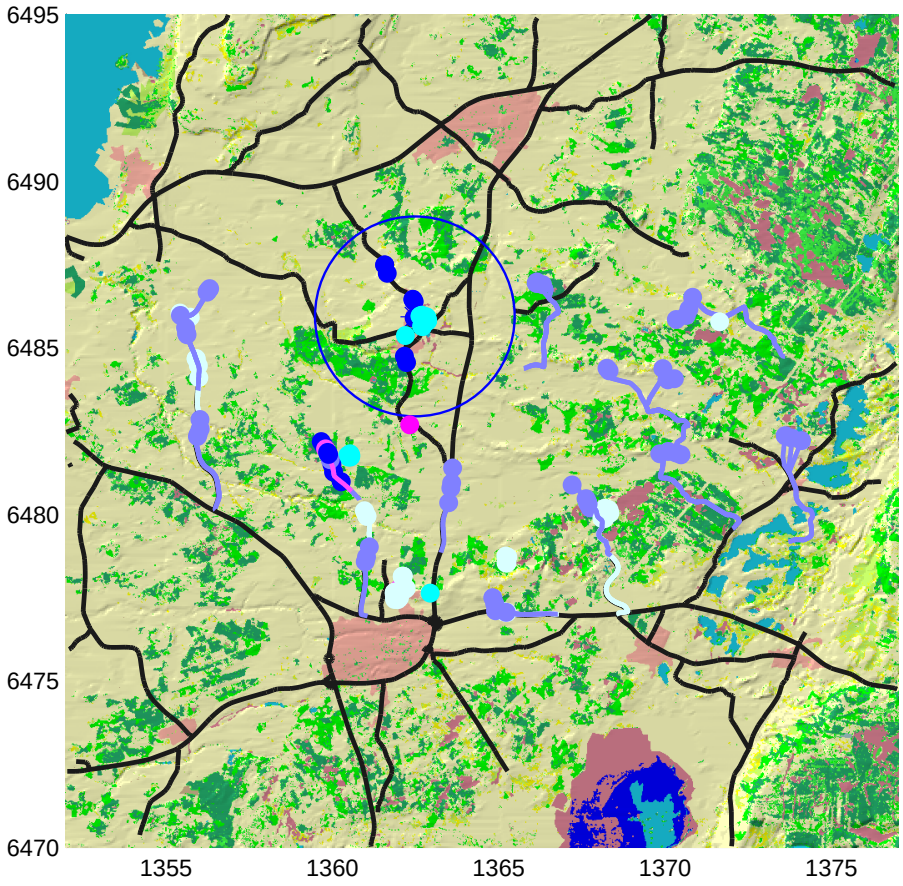


*Figure 3.6: Illustration of one nodes position information for the scenario where all nodes have intersystem interference corresponding to a computer at a distance of 10 m, F = 33 dB. The node of interest is in the middle of the **circle** which represents the 3 km perspective of the node. The {**blue**, **cyan**, **magenta**} dots represent {**fighting vehicles**, **non fighting vehicles**, **command vehicles at battalion level**}. Dots with a lighter colour of the colours above represent nodes with incorrect position information. The trails from this nodes ends in the correct positions.*

In Figure 3.5 we have plotted the positions for the scenario with no intersystem interference. As expected we can not se any errors. However, if we consider Figure 3.6 we can see some errors, especially in the east where the terrain is hillier.

## 3.5 Conclusions

From our simulations we conclude that intersystem interference in all units in a battalion can significantly reduce the availability of the SA service. We can also see that intersystem interference in only the command vehicles will only result in minor effects on the service availability. However, this reduction in service availability does not only affect the command vehicles, despite that they cause the intersystem interference.

The effects of intersystem interference might thus affect other nodes than the node that causes it. Hence, to analyse the effects of intersystem interference on a network and the services the network supports it is not sufficient to just analyse the communication link between two nodes. Instead we have to perform network simulations were the intersystem interference is incorporated to fully analyse the effect of intersystem interference.

# 4 EFFECTS OF INTERSYSTEM INTERFERENCE ON TRUST IN SA SERVICES FOR MECHANIZED BATTALIONS

## 4.1 Introduction

The preceding chapter shows that electromagnetic emissions from civilian equipment, such as a laptop, may interfere with the reception of radio communication in mechanized battalions. This interference decreases the range and/or data rate of the communication system which reduces the quality of SA services. The effects of the reduced quality on operators trust in the SA services were assessed in an initial evaluation.

First, the general characteristics of trust are described. Thereafter follows the mission objectives and organization of mechanized battalions. Finally, an initial evaluation of trust in the positioning service is described followed by some conclusions.

## 4.2 Characteristics of trust in SA services

The operators' trust in the communication system is very important for how they use and interpret the information from the SA services. Studies show that the more operators trust the system, the more they used it [15]. Therefore, operators that distrust the SA services will likely resort to using voice communication which is viewed as the main backup communication system in mechanized battalions [16]. Unfortunately, voice communication consumes considerably more bandwidth than the digital SA services for the same service levels. However, operators may also place to much trust in the SA services if they do not consider uncertainties that may affect the mission performance. Trust should thus be well calibrated to the actual capabilities of the SA services for the most efficient utilization.

Generally, trust can be considered as a way to reduce the perceived uncertainty in whether the information is correct, or a system or another person will perform as expected [17]. Continuously doubting the available information simply requires too much mental effort and hinders timely actions. Further, trust is achieved in a mental process that integrates experiences and observations of several system characteristics. Typical system characteristics may be persistence which allows the creation of mental models for prediction of future events, technical competence in the assumed role, and fiduciary responsibility when one has no experience of the service or can not evaluate the service [18]. Trust also develops over time in stages of predictability by evaluating the persistence characteristic, dependability from accumulated experiences of predictability in situations where the system may be unreliable, and faith by evaluating the responsibility characteristic [19]. High dependability and faith reduces the mental effort required to doubt the information. Unfortunately, terrain, interference etc. that may affect the quality of SA services are often not directly observable which may reduce the predictability of the

communication system. Overall, trust is affected by experiences and expectations about the future where all characteristics and stages are relevant to different degrees and dominate at different times. Early in a relationship, trust is based on available information but is later based on the experiences. Finally, all components of trust are integrated to a single perceived scale of trust [20].

Trust between humans and machines can generally be described with the same characteristics as trust between humans [21]. Theoretical frameworks that have been developed for trust between humans can therefore also be applied to human-machine trust. [21, 19] developed a widely used scale that utilizes this similarity for measuring human-machine trust. The scale was developed by combining the characteristics of trust from [18] and the stages of trust from [19]. For example, studies using this scale show that:

- Technical competence is the most important system characteristic for overall trust as can be expected [15].
- Predictability and dependability are the most important stages of trust development for overall trust [15]. The stages of trust development are even more important than the system characteristics for overall trust.
- Trust develops additively depending on the system's performance and the current trust [23].
- When trust is lost it takes a long time to recover partly because operators revert to manual control and use the system less [23].
- Interventions are affected by a combination of trust and self-confidence to perform actions manually [24]. Both the trust in the system and the self-confidence should therefore be well calibrated for best overall performance.

Trust is especially important for network centric warfare (NCW) and coalition operations where the partners may not have any previous experiences of working together. A research program about trust in NCW and coalition operations has therefore been established at FOI. Table 4.1 shows the dimensions of trust that were identified in the initial literature survey [25]. Military operators trust in SWAFRAP AJS, SWAFRAP C-130, CETRIS and command and control exercises have been studied using these dimension. Initial evaluations show that predictability, usability, robustness, and responsibility are important for the trust which is consistent with available theories [25].

| | |
|---|---|
| Predictability | Knowing how the system is going to react based on observations and experience |
| Capability | Capacity to function in situations that are important for the mission |
| Robustness | Ability to function when damaged or distorted |
| Familiarity | Similarity with previously used systems |
| Understanding | Knowing how the system "thinks" and operates |
| Usefulness | The system's practicality and applicability |
| Reliability | Functionality in difficult and dangerous situations |
| Dependability | The system's capability to fulfil its task in situations where it may be unreliable |
| Responsibility | The system is accountable and is not trying to blame others or find scapegoats |
| Intentionality | The system's purposes are congruent with the expectations, that is there are no hidden agendas |
| Transference | Trust is influenced by trust in other parts of the system |

*Table 4.1: Dimensions of trust*

## 4.3 Mechanized battalions

A mechanized battalion consists of about 1 000 men divided into three or four companies where each company consists of three or four platoons of three Mechanized Infantry Combat Vehicles (MICVs), or three Main Battle Tanks (MBTs). Each MICV carries an infantry group of six soldiers. The main mission objectives for a mechanized battalion is to take terrain or strike the opponent, although defence and delaying the opponent's advance are also important objectives. Strike is the most dynamic and offensive mission objective while defence and delaying the opponent's advance are more defensive. It takes about 12-24 h to delay the opponent's advance and the battle is mostly static, that is there are only few changes of combat positions.

Typically, the battalion is initially grouped over an area of about 100 $km^2$. They then advance for about 20 to 40 km towards the target with a speed of 300-500 m/min. There are high demands on coordination since all combat vehicles should reach the target at the same time. However, for strike against airborne troops, the battalion is initially grouped over an area of about 250-500 $km^2$ to maximize the area coverage. The maximum area coverage corresponds to a distance between the vehicles of about 3 km which is also the maximum distance for direct fire [6]. It is important to attack the landing zone as soon as possible before the opponent can regroup and form coordinated combat units. Usually, strike against airborne troops has less demands on coordination. Finally, other mission objectives are protect, hinder, support, march, and recover. When marching, the battalion is usually spread out on a long trail that is headed by a company and platoon that are around 500 m or 15 min ahead of the rest of the battalion.

| Type of unit | Strike | | Defence | Delay of advance |
|---|---|---|---|---|
| | Airborne ($km^2$) | Width x Depth | Width x Depth | Width x Depth |
| Mechanized battalion | 500 | 3-6 x 3 km | 5-10 x 3 km | 10 x 30 km |
| MICV company | 120 | 1.0-1.5 km | 2-3 x 1 km | 2-5 x 10 km |
| MICV platoon | 30 | 300 m | 500 m | NA |
| MICV | 10 | 100 m | 100 m | NA |
| MBT company | 120 | 1.5 km | 5 x 1 km | 5 x 15 km |
| MBT platoon | 30 | 300 m | 1 km | NA |
| MBT | 10 | 100 m | 100 m | NA |

*Table 4.2: Size of target areas for mission objectives*

Table 4.2 shows the size of the target areas for the most important mission objectives. Clearly, strike against airborne troop is the most challenging mission objective for a communication system.

The battalion is commanded by the staffs L1, L2, and L3. L3 is responsible for the strategic planning and L1 and L2 take turns in the tactical command and control that accompanies the strike movement. L3 also provides medical care, air defence systems, construction of trenches etc., and indirect fire. L3 consists of containers that are regrouped once every 24 h. L1 and L2, on the other hand, use MICVs that are especially equipped for command and control. Each command and control vehicle has six seats for the battalion commander, intelligence officer, artillery commander, combat commander, and two assistants. The battalion commander and intelligence officer are responsible of the overall planning. The intelligence officer integrates all target observations and creates a coherent description of the situation. The artillery and combat commanders, on the other hand, are responsible for the planning in a timescale of about 30-60 s. The battalion's command and control is generally directed towards the area coverage of the companies rather than individual vehicles. However, company commanders that are confronted with difficult situations may also receive support from the battalion's command and control about the location of specific vehicles.

The company commander uses a regular MICV. The company commander provides command and control for the company while concurrently participating in the battle. The company commander operates in a time scale of 10-30 s. The assistant company commander has his own MICV. Neither the company commander nor the assistant company commander have any infantry group. The timescale for platoon command and control and direct combat is a few seconds.

| Type of unit | Area coverage Width x Depth (m) | Fire distance (km) |
|---|---|---|
| Mortar platoon | 100 x 100 | 2-5 |
| Mortar company | 150 x 150 | 2-5 |
| Armoured mortar system | NA | 5-10 |
| Howitzer company | 150 x 225 | 10-25 |
| Howitzer battalion | 175 x 275 | 10-25 |
| 2 Howitzer battalions | 250 x 300 | 10-25 |
| >2 Howitzer battalions | 325 x 325 | 10-25 |

Table *4.3: Types of indirect fire*

| Command and control level | Timescale |
|---|---|
| Battalion | 30-60 s (area coverage) |
| Company | 10-30 s |
| Platoon | 1 s |
| Vehicle | 1 s |
| Indirect fire | 1-60 s |

*Table 4.4: Timescales for the command and control levels*

The artillery commander directs the indirect fire based on target observations from the companies or from fire control vehicles that specially equipped for precise measurements. Indirect fire can also be requested from the brigade. Table 4.3 shows the types of indirect fire. The timescale for indirect fire is about 1-60 s. Table 4.4 summarizes the timescales for the command and control levels.

The battalion supply company consist of medical care, maintenance, and air defence systems. The supply company use ambulances, five or six repair vehicles, bridge layer vehicles, and three air defence vehicles. The air defence vehicles follows the movement of the combat force. The rest of the supply company only regroup every 12 or 24 h. The supply units for each company consists of medical care and maintenance with only one repair vehicle.

## 4.4 Positioning service for mechanized battalions

The positioning service for the location of other units in the battalion is an important SA service. Generally, about 70 % of the voice communication consists of position information [26]. Therefore, it is not surprising that operators perceive the positioning service as the best SA service [16]. The purposes of the positioning service is to avoid fratricide and to facilitate coordination during battle. The positioning service also has indirect functions, such as to provide an understanding of the progress of the battle and to localize likely opponent positions. Avoiding fratricide requires very small position errors of less than 20 m for all vehicles that are within the range of direct fire, that is 3 km. The requirements on position error decreases when the timescale increases. For battalion command and control that is more concerned with companies area coverage, a position

error of a few hundred meters does not matter [27]. The emergency vehicles of the supply company have the least requirements on position error, although they need accurate position information of where the others are for coverage and to avoid hostile fire.

Only the requirements for avoiding fratricide and the companies area coverage were considered for further evaluation based on discussions with subject matter experts (SME). The preceding chapter shows that the position errors of 20 m for fast moving vehicles within 3 km range corresponds to a time delay of 1 s in position updates. Similarly, a position error of a few hundred meters for the companies area coverage corresponds to a time delay of about 10 s in the position updates. However, in SLB, a Swedish SA service for mechanized battalions, the lack of position updates are only indicated with a discrete symbology change after 30 s [27]. 30 s can therefore be seen as the upper limit for any acceptable delays. A dependent measure of the position error for the companies area coverage was developed by enclosing the combat units in a company within a convex hull similar to those used in SLB [28]. The hulls were interpolated in small steps to allow more detailed measurements. The position error was measured by finding the point on the convex hull for the correct position that was closest to target area in the lower right corner and measuring the distance to the closest position on the estimated convex hull. Figure 4.1 illustrates the principle for measuring the position error of convex hulls. The maximum position error of the convex hulls for the four companies was then selected as the measured position error.

The simulation results in the preceding chapter shows that the data rate and level of interference interact in the service availability for avoiding fratricide. When the data rate and level of interference increases the service availability decreases. Generally, the command and control vehicles are slightly more affected than the rest of the battalion. The results indicate that even when only the command and control vehicles are affected by 44 dB interference (see section 3.4 for an explanation of the interference levels), there are occasions with 2.0 Mbit/s data rate when the delay in position updates for is longer than 30 s although the service availability is very high. When the interference affect all vehicles, there can be considerable delays both at 33 and 44 dB interference for all data rates. However, these delays may well be due to terrain coverage where there is no risk for fratricide. Therefore, some form of line of sight indication has to be included for further evaluation of the risk for fratricide.

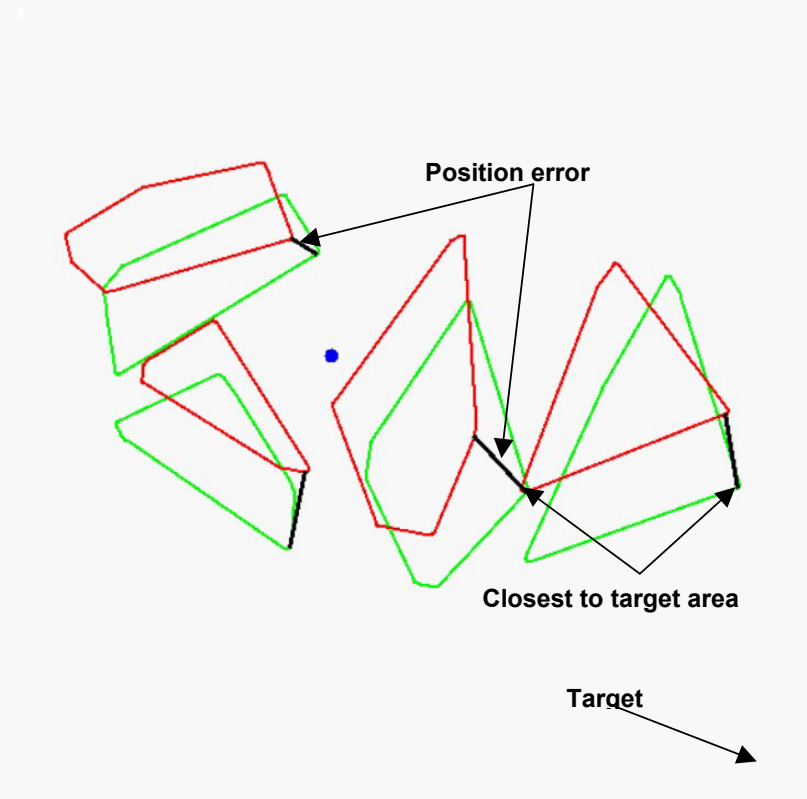


*Figure 4.1: Principle for measuring position error of convex hulls*

Figure 4.2 to Figure 4.4 shows the calculated position error for the companies convex hulls for L1, L2, and L3 at 0.5 Mbit/s data rate when the interference affects all vehicles. All figures show a similar effect where even 22 dB interference can cause position errors up to 1 km. These position errors are clearly higher than the few hundred meters of acceptable position error that was suggested by SMEs. Even if the position errors are not significant in themselves, there is a considerable variability that reduces the predictability of the positioning service. At 33 dB interference the position error can be up to 5 km but is gradually reduced as the units converge on the target area. At 44 dB interference the position error increases more or less continuously during the whole scenario. The preceding chapters shows that for units beyond 3 km, which are the main basis for convex hulls, the delays for 33 and 44 dB interference can be several minutes. Clearly, interferences of 33 and 44 dB causes position errors that may hamper the battalion commanders ability to control the companies. This may of course reduce the trust in the positioning service. Finally, since L3 is stationery, it is surprising that the position error is not worse than for L1 and L2 who follows the companies towards to target area. This may, however, be an effect of the initial positions in the current scenario.

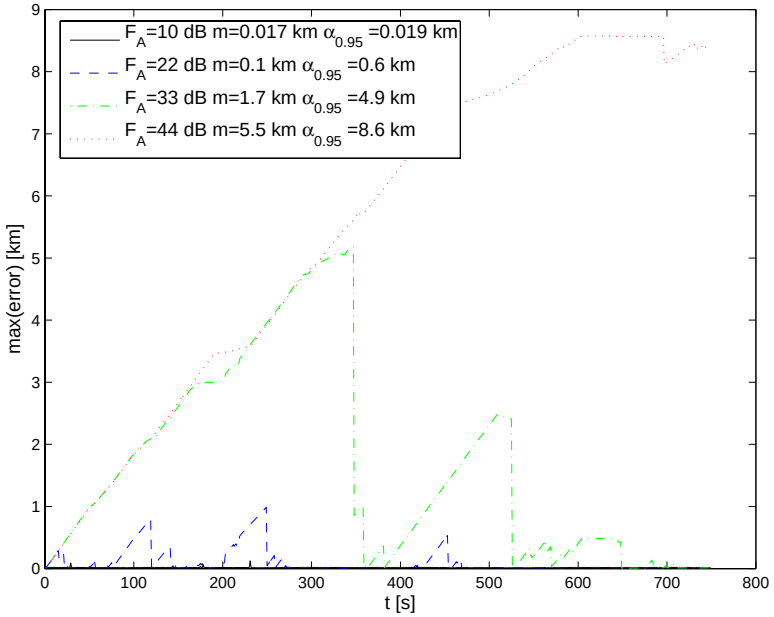


*Figure 4.2: Maximum position error of the companies area coverage for L1 at 0.5 Mbit/s data rate. The mean position error over the scenario is shown in the legend. The mean position error was calculated by excluding the 95 % percentile.*

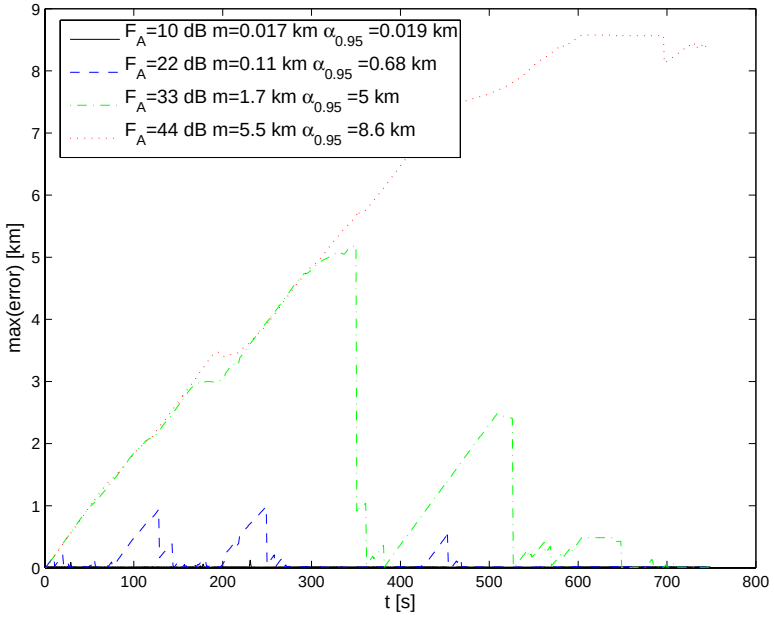


*Figure 4.3: Maximum position error of the companies area coverage for L2 at 0.5 Mbit/s data rate. The mean position error over the scenario is shown in the legend. The mean position error was calculated by excluding the 95 % percentile.*

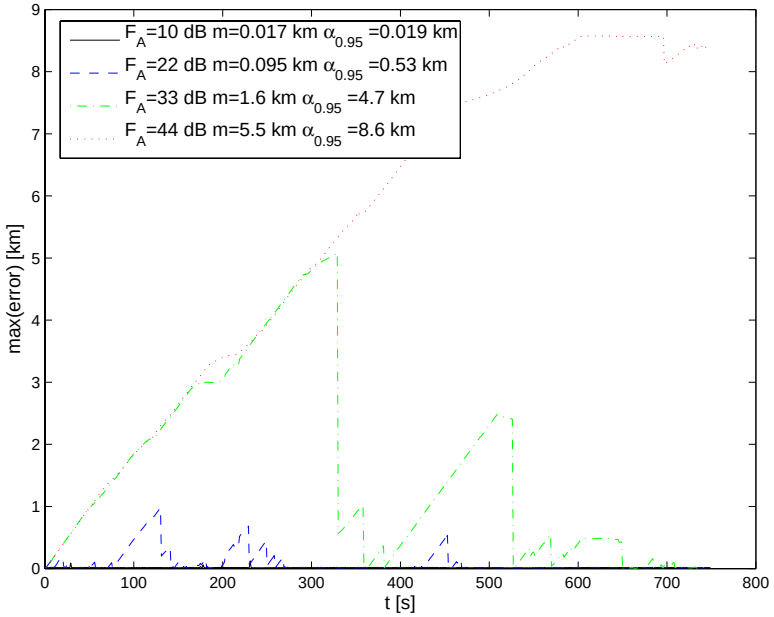


*Figure 4.4: Maximum position error of the companies area coverage for L3 at 0.5 Mbit/s data rate. The mean position error over the scenario is shown in the legend. The mean position error was calculated by excluding the 95 % percentile.*

## 4.5 Conclusions

The results show that even for low data rates and levels of interference that affect all vehicles, there are situations where the battalion commander may not have sufficient position information about the companies area coverage. Even if the position errors are not significant in themselves, there is a considerable variability that reduces the predictability of the positioning service. Especially since the source of the variability, such as terrain and interference, may not be directly observable. Further, the theoretical discussion shows that the reduced predictability may also affect other characteristics of trust, such as the perceived dependability. When the interference increases further, the position error becomes unacceptable. Position errors over 1 km in the command and control vehicles for the companies area coverage clearly hampers the battalion commanders ability to control the companies. Further research is required to establish how the position errors and the variability affect the operators' trust in SA services. Preferably, by asking SMEs for subjective ratings of how they experience the SA services on an appropriate scale of trust.

The results indicate there may be situations were high interference increases the risk for fratricide. However, the risk should be interpreted cautiously until a line of sight measure has been included in the analysis. A further analysis may also compare the battalion commanders position information with the company commanders position information for an

assessment of the potential for confusion when the company commanders receive support about the location of specific vehicles. Such an analysis may also benefit from using distributions of time delays as the common method of comparison.

# 5 INTERSYSTEM-INTERFERENCE RISKS AND EMERGING TECHNOLOGIES

## 5.1 Introduction

In this chapter, intersystem interference risks due to coming technology solutions are discussed. The development of new technologies within the area of wireless systems is extremely rapid and this opens up several new possibilities for the future military defence in the development of systems for C4ISR. The development within the commercial area will have a great influence on future military systems since the Swedish defence is obliged to use standardised commercial products and components whenever feasible. In this chapter, different aspects of technology trends are described and discussed from an intersystem-interference perspective. A ranking of these intersystem-interference risks is then presented in Chapter 6.

## 5.2 Commercial off the Shelf (COTS) Technology

The development towards a Network-Based Defence (NBD) contains a lot of challenges both for the armed forces and the industries involved. One key area is how to link together different military functions, such as decision making, information systems and weapon systems, in a single networked organization. Another key area is how to do this with reduced defence budgets and high technical demands on the command & control systems involved. A possible solution is to use an increased amount of commercial off the shelf equipment (COTS) in the military defence. The reason is that the technological advances in the commercial electronics industry are extremely rapid. These developments are largely based on the demands and possibilities of civilian society. This is a situation that will also, to a large extent, guide military development and the feasibility of designing command and control systems within the armed forces in years to come. From a historical point of view, military technology has always retained a pole position in the application of new technology. This was the situation during the days of the cold war. In the current situation, the technical developments on the civilian market have caught up on the military technology in a number of fields and especially within telecommunications and information technology. Together with the reduced defence budgets, this situation opens up completely new possibilities for the armed forces to use civilian electronics in military applications. To do this in a successful way, it is important to be aware of some fundamental properties of COTS. As COTS is developed for other customers than military forces, it has some limiting properties that must be taken care of in order to use it as an efficient part of modern military command & control systems.

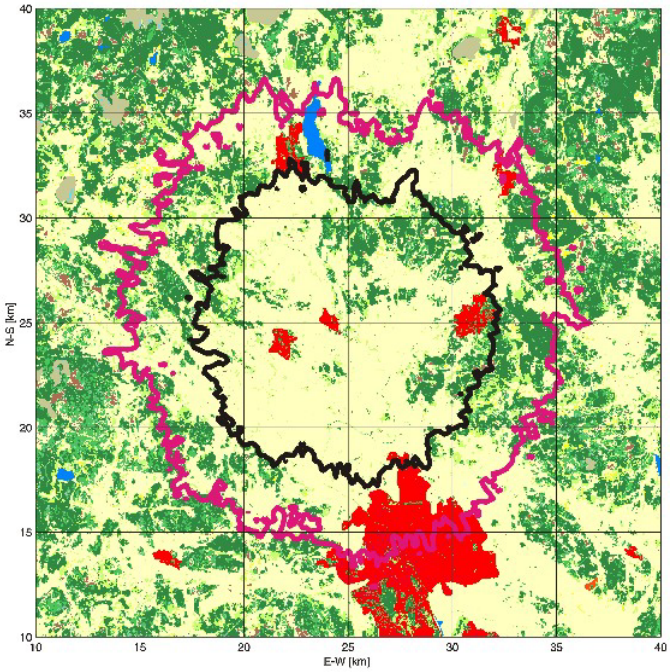


*Figure 5.1: The operating range is reduced due to interference from co-located COTS equipment. Red colour is the operating range with no intersystem-interference present.*

One important property to be aware of is that COTS contribute with more electromagnetic interference than military specified equipment does. In this report the abbreviation COTS is therefore defined as "electronic equipment satisfying civilian radiated emission standards".

One reason why commercial electronics are cheaper than military is due to that commercial equipment is allowed to radiate considerably higher levels of unwanted electromagnetic interference than military specified equipment. This interference can severely degrade the performance of co-located military wireless communication systems. Simulations and measurements of performance degradation have shown that the operating range of wireless army combat radios can be reduced to 25-50% if co-located with COTS at distances of 10-20 meters [34]. In Figure 5.1 the operating range for a frequency-hopping (30-88 MHz) army combat radio is simulated with and without co-located COTS equipment. The COTS equipment consists of some personal computers with an electromagnetic emission spectrum approved for sale in the European Union. The co-located radio system is located in the centre of the figure (of size 30x30 km) and 20 meters from the COTS equipment. The radio system is supposed to be used for transmission of speech with a requirement on the bit-error probability of <10-3.

## 5.3 Unmanned (Combat) Aerial Vehicles, UAV/UCAV

Unmanned Aerial Vehicles (UAVs) are presently being utilized by several countries for reconnaissance, surveillance, target location and battle damage assessment. In the future, UAVs are proposed as an alternative to manned aircraft for missions characterized by the three Ds: dull, dirty, and dangerous. Dull means long-endurance missions which may become as long as several days due to the desired range and loiter time of the system. Dirty refers to operating in an environment that is contaminated by chemical, biological or nuclear agents. Dangerous missions include suppression of enemy air defence or other missions that require operation in high-risk areas. In a reconnaissance capacity, UAVs fill a gap between satellites and manned reconnaissance flights. Satellite technology, though advanced, is logistically and economically unfeasible in situations requiring spot reconnaissance. Manned aircraft, on the other hand, cannot loiter and focus on a particular spot for long stretches of time as they are susceptible to hostile fire. This has opened up for a frequently use of UAVs. UCAVs is a further development of UAVs. UCAVs are also equipped with weapon systems. The development and deployment of UCAVs is believed to significantly increase the effectiveness and survivability of manned fighter aircraft while lowering the overall cost of combat operations. Because of their small size, lack of pilot interfaces and training requirements, reusability and long-term storage capability, UCAVs are projected to cost up to 65 percent less to produce than future manned fighter aircraft, and up to 75 percent less to operate and maintain than current systems.

Since the size of a UAV can be very small, the distance between on-board transmitting and receiving antennas will be very small. The combination of remote flying and a large amount of systems for reconnaissance increases the risk for intersystem interference both between on-board systems and with other users of the electromagnetic spectrum. A typical UAV system contains e.g. radio relay links, data links, satellite data links and synthetic aperture radar. In a test flight over a range in the southwest United States, a Global Hawk Unmanned Aerial Vehicle (UAV) experienced interference from an adjacent test range that was testing auto-termination transmissions on the same frequency. The result was initiation of the self-destruct mechanism in the UAV; the aircraft was destroyed [1].

## 5.4 Multi-Role/Purpose Platforms

An increased use of platforms designed for multi-roles or multi-purposes could be the reality in the future. In this context we mean multi-role platforms with significant different user profiles such as platforms combined for jamming and signal intelligence STEJL (Swedish abbreviation for “Störning Pejl”), or modularised platforms such as SEP (Swedish abbreviation for the Alvis/Hägglunds “Splitterskyddad EnhetsPlattform”, Modular Armoured Tactical System). Such platforms are for instance characterized by low signature, high mobility, high flexibility and high reliability. From an intersystem-interference point of

view, multi-role platforms are in general of high interest. The multi-role ability typically requires wireless systems that need to transmit and listen at the same frequencies at the same time. A typical example is the ability to perform signal intelligence*), jamming and reconnaissance*) at the same time. Thus, multi-role platforms are judged to be more vulnerable to intersystem-interference problems than platforms dedicated for one specific purpose.

*) [35].

## 5.5 Dynamic Spectrum Access (DSA)

Currently the assignment of spectrum to different radio systems is based on fixed allocations, where the spectrum is divided into non-overlapping blocks assigned to different radio standards, separated by guard bands. Whilst effective at managing interference, this has the disadvantage of allowing spectrum to become unused at certain times or in certain areas, as the demands for the spectrum from the networks vary. It takes many years to arrange the harmonized frequency allocations needed by services such as GSM or UMTS, and during this time spectrum is unused - and sometimes planned services are never set up. Similarly, at the end of the service's life, spectrum can lie dormant until a new use is negotiated. The currently used mechanisms for spectrum management are believed to be a contributing factor to the long lead times from innovation to market in wireless technologies and systems. This has in turn been a major contributing factor to the dominance of the large telecom companies in the European and World markets, whereas very few innovative enterprises have exhibited constant growth, although the technical competence in Sweden is very high in this area. Alternative spectrum management regimes, such as the introduction of "unlicensed bands" have proven very effective in lowering entry thresholds for smaller companies (e.g the WLAN business). In addition, experts claim that the spectrum requirements for communication purposes will increase by as much as 200-300 % up to 2010. At the same time the actual usage of the electromagnetic spectrum is very inefficient. This motivates the investigation of a more flexible and spectrum efficient technique called dynamic spectrum access (DSA) [37].

Dynamic spectrum access focuses on the design and evaluation of algorithms that share the spectrum between several radio systems or radio access networks (RANs). This means a spectrum allocation method that adapt to changing demands for the spectrum, either over time, space, or both. However, there are two major obstacles to overcome. First, as the same block of spectrum could be used by different RANs in neighbouring areas, the management of intersystem interference is vital. Second, the size of spectrum management areas is important. When the areas are large there is less difference in spectrum use between them and hence less advantage to be gained. When the areas are small the effects of intersystem interference become harder to manage.

Thus, one key issue is to find reliable methods and algorithms for intersystem interference control between different users of the same spectrum. This will require new methods for dynamic intersystem interference control that can be used more or less on line. Intersystem interference is the most difficult of the technical problems that have to be solved. Thus, with DSA it is likely to assume that new intersystem interference problems will occur. DSA can therefore be regarded as a technology that will increase the risk for future intersystem-interference problems. It is difficult to judge whether DSA will be a reality or not in the future. Several actors in the United States argue for a more dynamic frequency allocation politics so that unused or underused spectrum can be more effectively used. The telecommunications industry is one contributing actor. Furthermore, in April 2004, the IEEE-USA recommends the FCC to explore the potential of dynamic radio systems to facilitate the sharing of unused or underused spectrum. It is however reasonable to assume that DSA will not be a reality within the coming ten years since all processes connected to spectrum allocation tend to take very long times to handle.

Several major evolutions of present analysis methods for intersystem interference are needed in general for dynamic spectrum access:

- Intersystem interference analysis methods for on-line (on-demand) use must be developed to handle dynamic changes both in space (physical location) and time.
- Analysis methods for a reduced number of in-going system parameters must be developed.
- Analysis methods that can aid the prediction of consequences on a higher system level than separate links are needed.
- Current spectrum policies are based on “interference-limited” rather than “ambient noise-limited” environments. “Interference limited” means that only other users are considered in the intersystem-interference analysis. In a dynamic network scenario the total environment must be considered which requires new methods that are “ambient-noise limited”.

DSA can be implemented in different ways or concepts. Independent of the exact DSA concept chosen, there are several fundamental research problems that must be solved concerning dynamic spectrum interference control. Furthermore, depending on DSA concept chosen, different specific technical problems will appear. It is however difficult at this stage to judge which of these concept-specific problems will be of most importance to solve.

The FCC has released a “Notice of Inquiry” and “Notice of Proposed Rulemaking” seeking to use an "interference temperature" model for quantifying and managing radio frequency interference. In contrast to the Commission’s current method, which is based on transmitter operations, the interference temperature metric focuses on the actual RF environment surrounding receivers. Under this approach, new devices would be

permitted to operate in a band if their operation does not cause overall emissions in the band to exceed a preset limit. One difficulty with such approach is that the waveform, not only the power, of an interfering signal can significantly affect the performance of a disturbed system. This is a well known result in intersystem-interference research. Thus, this metric could be too blunt and must be further investigated to determine the risks of under/overestimation the interference impact if used.

In the following, intersystem-interference research questions of fundamental importance for dynamic spectrum access are identified.

- Investigation of convenient decision metrics for intersystem interference control online. What kind of interference measurements (metrics) is convenient for instant decision making online? Convenience includes both parameters that give relevant information of the interference impact and parameters that are convenient for practical implementation in systems. Is for instance the "interference temperature" a convenient metric although the interfering waveforms are not considered in that metric?
- What overall system performance properties should have most influence on the final decisions given a certain convenient interference metric? Several alternative performance properties could be of interest such as QoS, reliability, capacity etc.
- What metrics are convenient in order to control that given rules are followed by the users?

## 5.6 Software Defined Radios (SDR)

Software Defined Radios are elements of a wireless network whose operational modes can be changed or augmented, post-manufacturing, via software. They use adaptable software and flexible hardware platforms to address the problems that arise from the constant evolution and technical innovation in the wireless industry particularly as waveforms, modulation techniques, protocols, services, and standards change. A software defined radio in the SDR Forum [29] context goes beyond the bounds of traditional radio and extends from the radio terminal of the subscriber, through and beyond the network infrastructures and supporting subsystems and systems, to access not only other users, but suppliers of value-added applications. SDR as a concept spans numerous radio network technologies and services, including cellular, PCS, broadband wireless, WLANS, mobile data, emergency services, messaging, paging, and military and government communications.

Software defined radio is a complex topic involving many aspects including radio aspects, network aspects, and spectrum efficiency considerations. There is a need for specific recommendations in regard to SDR because of the technology's potential for spectrum enhancement. Software defined radios with flexible RF front ends provide multimode, multi-band capabilities. This provides the possibility of sharing spectrum between different operators on a flexible, real-time basis. This requires

mechanisms for jointly managing the radio resource and the spectrum resource. Spectrum can be shared between service providers based on real-time needs of the service providers in a given geographical area. All of above is predicated on the establishment of an evolutionary regulatory environment. Regulatory issues must be resolved before reconfigurable radio is brought into the marketplace. The Software Communications Architecture (SCA) is a set of rules for deploying and interconnecting the signal processing objects of a software defined radio (SDR) system. The U.S. Department of Defense's Joint Tactical Radio Systems (JTRS) Joint Program Office is focusing on the SCA as a key enabler for developing versatile, interoperable SDR systems. These systems are expected to improve the ability of warfighters to communicate on modern battlefields, and also deliver important benefits for users outside the military.

Technologies such as software-defined radios are sometimes called "smart" or "opportunistic" technologies because in the future they may search the radio spectrum, sense the environment, and operate in spectrum not in use by others. By operating in so-called white – or unused –spaces in the spectrum, software-defined radios could enable better and more intensive use of the radio spectrum. Smart technologies, such as software-defined radios, potentially allow operators to take advantage of the time dimension of the radio spectrum. That is, because their operations are so agile and can be changed nearly instantaneously, they can operate for short periods of time in unused spectrum. However, this capability is a future capability that has implications on the network as well as the radio. Achieving this potential benefit for software-defined radio requires advances in spectrum management, network control, as well as the software-defined radio itself. It also requires changes in the way that regulators have assigned spectrum. Historically, due in large part to technological limitations in radio performance, regulators have assigned spectrum according to particular operational frequencies and geographic areas of operations. In the future, as network control and spectrum management capabilities associated with SDR are developed, this spectrum assigned model may need to be re-examined. Thus, DSA is necessary in order to use the full potential of SDR. Another way of seeing this relationship is to see SDR as the necessary technology to use DSA. SDR can therefore be regarded as a technology that will increase the risk for future intersystem-interference problems. Software defined radios are already being developed and the first deliveries is expected to take place approximately around year 2007 in the JTRS project [30].

## 5.7 Smart Antennas

A smart antenna system combines multiple antenna elements with a signal-processing capability to optimise its radiation and/or reception pattern automatically in response to the signal environment. The concept of using multiple antennas and innovative signal processing to serve cells more intelligently has existed for many years. In fact, varying degrees of relatively costly smart antenna systems have already been applied in

defence systems. Until recent years, cost barriers have prevented their use in commercial systems. The advent of powerful low-cost digital signal processors (DSPs), general-purpose processors (and ASICs), as well as innovative software-based signal-processing techniques (algorithms) have made intelligent antennas practical for cellular communications systems. Today, when spectrally efficient solutions are increasingly a business imperative, these systems are providing greater coverage area for each cell site, higher rejection of interference, and substantial capacity improvements.

Smart antennas will probably be more widely used in future military and civilian wireless applications. The main purpose with these antennas is to be able to change the antenna pattern with means of signal processing. Adaptive antenna technology represents the most advanced smart antenna approach to date. Using a variety of new signal-processing algorithms, the adaptive system takes advantage of its ability to effectively locate and track various types of signals to dynamically minimize interference and maximize intended signal reception. These systems attempt to increase gain according to the location of the user and provide optimal gain while simultaneously identifying, tracking, and minimizing interfering signals. This technology opens up for the possibility to use the same frequency in different directions or to decrease the antenna gain in the direction of a hostile jammer.

The drawback with this technology is that intersystem interference can affect the antenna pattern in an unpredictable way. If intersystem interference is interpreted as hostile jamming, the smart antenna starts to decrease the antenna gain in that direction. Since intersystem interference can occur in the same direction as other legal systems, this effect can decrease the overall performance of a communication network. There is always a limited number of directions in which a smart antenna can decrease its antenna gain. Therefore, if the number of intersystem-interference directions is equal to or larger than this limited number, the antenna pattern will change in unpredictable ways and severely degrade the overall system performance. In Figure 5.2, an example of how intersystem interference, represented by COTS equipment, can affect the antenna pattern is shown [32]. Green line is the direction towards the legal system, whereas red lines refer to the directions to hostile jammers. Upper and lower frequencies for the radio system are denoted with black and blue lines respectively. In Figure 5.2, the antenna system can handle the intersystem interference and at the same time create a high antenna gain in the direction to the legal system. In Figure 5.3 the intersystem interference causes the antenna gain in the direction to the legal system to decrease considerably. However, even if the smart antenna is subjected to intersystem-interference its performance is in several cases better than for a static antenna.

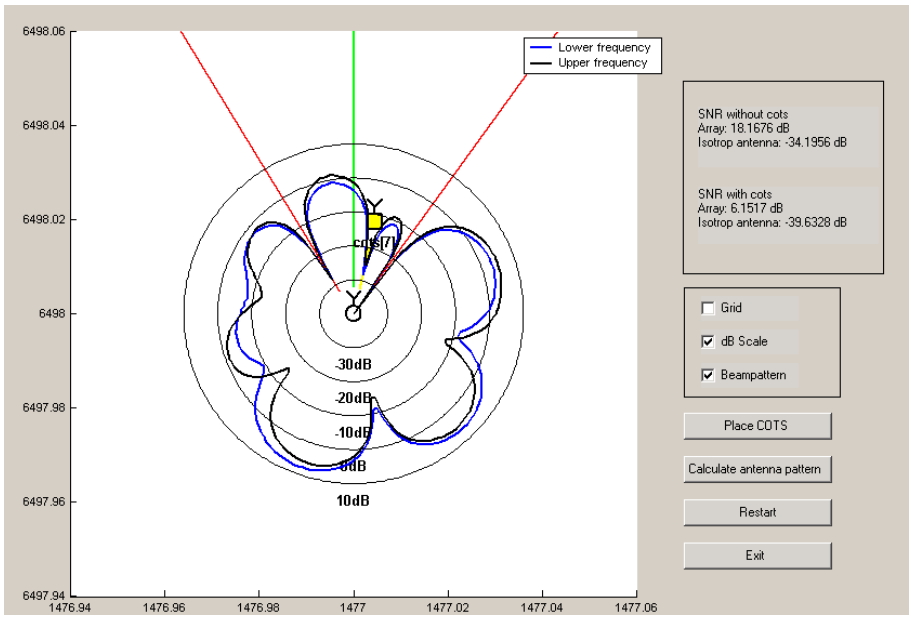


*Figure 5.2: The antenna can handle the intersystem interference from the COTS equipment.*

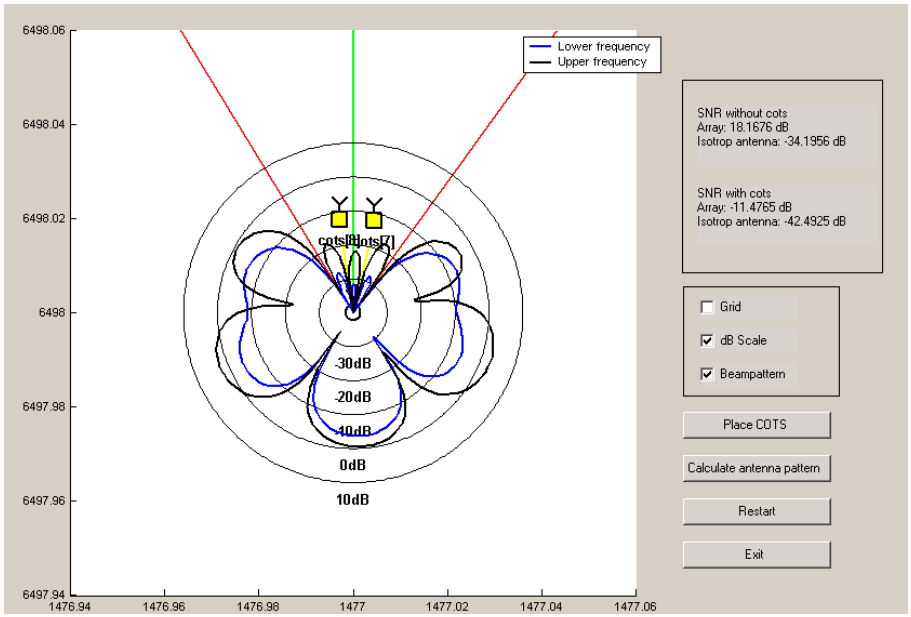


*Figure 5.3: The antenna diagram is severely affected of intersystem interference.*

## 5.8 Ultra Wide Band (UWB) Technology

Ultra-Wideband (UWB) technology is generally defined as a wireless transmission scheme that occupies a bandwidth of more than 25% of a centre frequency, or more than 1.5 GHz. UWB has been around since the 80s but it has been mainly used for radar-based applications, as the wideband nature of the signal provided accurate timing information (due to the inverse relationship between the time and frequency response of an electrical signal). However, the advances in the high-switching technology are now making UWB more attractive for consumer communication applications. The existing aspect of UWB is that, by spreading data across a large swathe of the electromagnetic spectrum, wireless communications could theoretically approach data rates of 1 Gbit/s over short distances. With signals that are so highly spread, the energy level in any given part of the spectrum is low enough not to interfere with established services, proponents claim. However, even if UWB does not knock out established services, it would manifest itself as an increase in the background noise. Such increase can give detrimental impact on the electromagnetic spectrum since any increase will add to all other existing background noise components.

In 2002 the FCC (Federal Communications Commission) decided to allocate 7500 MHz of unlicensed spectrum for UWB communications in the 3.1 GHz to 10.6 GHz frequency band. By April 2003, the 802.15a working group received an unparalleled 23 proposals for dividing this 7.5 GHz of spectrum. This multi-band approach would divide the 7.5 GHz of spectrum into smaller, typically 15 sub bands of 500 to 700 MHz that would be added or dropped depending on interference from other systems. However, this approach leaves the original UWB concept since it will require that the signal is modulated into narrower frequency bands. There is already a well-known and deployed spread-spectrum technique for transmitting data in arbitrary limited frequency bands. This technique is OFDM (orthogonal frequency division multiplexing) which offers the possibility of shifting data onto the most appropriate channels, while it creates and suffers from the least interference. Thus, it is likely to assume that this multi-band approach will lose the original benefits of the UWB technique and favour the well-established OFDM technique instead [31]. However, a probable solution could be different kinds of hybrid UWB/OFDM techniques to handle the multi-band approach.

# 6 RANKING OF FUTURE INTERSYSTEM-INTERFERENCE RISKS

In Table 6.1, the discussions in the previous chapters are summarized together with a judgement of the intersystem-interference risks. The time perspective for when the different issues are expected to be a reality is also judged in the table. The table headings should be interpreted as follows.

**Issue** — Brief description of the issue causing the risk.

**Consequence** — Brief description of the consequence from an intersystem interference perspective.

**Risk for intersystem-interference problems** — A judgement of the risk of that intersystem interference problems will occur due to the issue.

**Probability to occur** — A rough judgement of the risk that the issue itself will be a reality.

**Time perspective** — A judgement of when the issue is likely to be a reality in the future.

| Issue | Consequence | Risk for Intersys. Interfer. problems | Prob. to occur. | Time pers-pective |
|---|---|---|---|---|
| Increased use of COTS*) | In general higher electromagnetic interference levels | High | High | <5 years |
| Joint operations between military and civilian units at national level | Unpredictable co-location situations between military and civilian wireless systems. | High | High | >10 years |
| Joint operations between different military units at national level | Unpredictable co-location situations between military wireless systems. | Medium | High | 5-10 years |
| Combined operations, international level | Unpredictable co-location situations between military wireless systems from different nations. Requirement on systems for | High | High | <5 years |

| | | | | |
|---|---|---|---|---|
| | interoperability with international civilian units (e.g. warships must be equipped with civilian systems for identification and communication). Lack of available frequencies during these operations severely degrades robustness for frequency-hopping systems. | | | |
| Compact platforms (e.g. UAV, UCAV) | More systems per area unit | Medium | Medium | >10 years |
| Multi-role platforms (e.g. SEP, STEJL) | Large amount of transmitting and receiving wireless systems. | Medium | Medium | >10 years |
| Dynamic Spectrum access | Unpredictable electromagnetic environment. Methods for intersystem interference analyses on line must be developed. | High | Medium | >10 years |
| Software defined radios | Unpredictable electromagnetic environment. Methods for intersystem interference analyses on line must be developed. | High | High | <5 years |
| Mobile ad-hoc networks | Unpredictable effects on higher system levels e.g. if wireless SA services are disturbed. | Medium | High | 5-10 years |
| Broad-band antennas | Increased sensitivity for interference in wide frequency bands. | High | High | 5-10 years |
| Smart antennas | Unpredictable impact on beam-forming algorithms | High | High | 5-10 years |
| UWB systems | Increased noise levels in wide frequency bands | High | Low | >10 years |

***Table 6.1:*** *Ranking of some intersystem-interference risks.*

*) In this report the abbreviation COTS is defined as “electronic equipment satisfying civilian radiated emission limits”.

# 7 CAPABILITIES OF PRESENT INTERSYSTEM INTERFERENCE ANALYSIS METHODS

The background of intersystem interference analyses may be found in the 1920s, when broadcasting services started to reach the general public. Quite soon it became evident that control of the generation of different man-made radio disturbances was essential in order to guarantee a good quality of the new broadcasting services. However, imposing limitations on electrical equipment and household appliances could cause trading problems if different countries applied significantly different norms. This problem was soon realized on national levels, which led to the foundation of the International Special Committee on Radio Interference (C.I.S.P.R.). The International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) were cofounders [36]. The first goal was to reach an agreement on measurement procedures. This work was carried out during the 1930s. After that, the work of developing standard emission limits could start. The first standard produced was at a national level when the BS613 (1935) concerning components for radio disturbance suppression devices was published in England. In 1937, the BS727 concerning characteristics of an apparatus for measuring of radio disturbance was published. This standard had a major impact on the standardization work within C.I.S.P.R. The C.I.S.P.R. Publication No. 1 including the characteristics of a standardized measurement receiver and certain design features was published in 1961. In the practical applications, man-made disturbance sources have up to now been divided into two major categories with its own methods and approaches; intentional and unintentional sources. Intentional sources include other transmitting equipment which typically works with some kind of modulated signals and whose disturbance typically consists of harmonics and intermodulation products. Unintentional sources are other electronic systems that are not intended to produce any radiated electromagnetic energy and whose electromagnetic energy typically consists of different kinds of electromagnetic noise such as Gaussian noise and impulse noise. Historically, the work of analysing radio-interference problems has been carried out in three separate areas of application:

- Frequency planning
- Intersystem-interference analyses for intentional sources.
- Intersystem-interference analyses for unintentional sources

Each of these areas has its own methods to comply with the different applications of the analyses. In general, existing state-of-the-art analysis methods for intersystem interference are based on algorithms for analog systems, modified with simplified algorithms to analyse the impact on digital communication receivers. The underlying algorithms for analog systems require detailed information of the systems analysed. System parameters not specified in the system specification are assumed to be determined by additional measurements. These kinds of measurements are normally very expensive to perform and therefore the needs for new

analysis methods that do not need such detailed information have been recognized. No such methods have yet been published.

In existing algorithms, the intersystem-interference analyses of digital systems are based upon the simplification that all interference signals are treated as if they were additive white Gaussian noise (AWGN). This means that only the power, not the waveform, of the interference signal is considered to estimate the impact on a digital radio receiver. The main reason for this simplified approach is that alternative methods are much more complex and requires more powerful analysis tools and more skilled personnel to use them and interpret the results. One drawback with this simplified approach is that the waveform of an interference signal dramatically affects the impact on a digital system. Unfortunately, for some interference signals, this approach significantly underestimates the impact on a digital communication system [33]. The rapid development within the area of digital communications has given an increased variety of system parameters that an analysis tool must be able to handle.

The development of analysis tools for intersystem-interference analysis has not been fast enough to handle all new digital systems in another way than with simplified models. This phenomenon is schematically illustrated in Figure 7.1. Furthermore, existing analysis methods are designed to analyse static scenarios both in space and time, i.e. the analyses are performed for a limited amount of interference-victim combinations. In summary, the state of the art within intersystem interference analyses could be described as follows:

- Present methods/tools for intersystem-interference analyses are based on algorithms for analog systems, modified with simplified algorithms to analyse the impact on digital communication receivers. These simplified methods that do not consider the interference waveform properties are widely used.
- The analyses are done for static scenarios in space for a limited number of transmitters and receivers. The focus is on the transmission/receiver link levels and the final result is obtained by worst-case assumptions where the simultaneous impact from different interference sources is considered.

In present methods the underlying models for analog systems require detailed knowledge of system parameters.

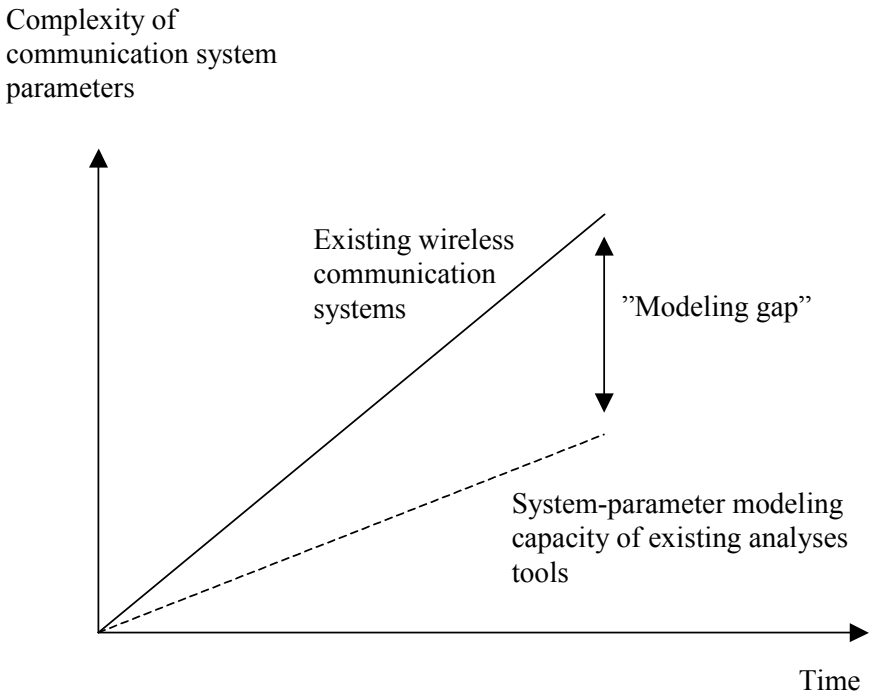


*Figure 7.1: A schematic view showing that the capacity to handle the increasing amount of system parameters is to low in existing analysis tools for intersystem interference.*

# 8 NECESSARY CAPABILITIES OF FUTURE ANALYSIS TOOLS

Examples of challenging new research domains within intersystem interference have been described and discussed in this report. The underlying driving force for the domains is the emerging software defined radio and cognitive radio technologies for dynamic and flexible systems. These domains require completely new analysis methods since the interference effects appear as higher-order effects on system-of-system levels and on human factors. Furthermore, it is important to consider the total ambient environment to provide reliable results of the intersystem-interference analyses for these coming systems. These interference analyses cannot be solved with traditional intersystem-interference analysis methods. Analysis methods that can aid the prediction of consequences on a higher system level and human factors in dynamic systems are needed. We are here facing the problem of dynamic interference control or dynamic interference avoidance.

In summary, the needs on new analysis tools for intersystem-interference analyses are the following.

- Intersystem interference analysis methods for on-line (on-demand) use must be developed to handle dynamic changes both in space (physical location) and time.
- Analysis methods for a reduced number of in-going system parameters must be developed.
- Intersystem interference analysis methods that include the total electromagnetic environment, e.g. ambient noise, must be developed in order to provide reliable results for the coming wireless systems.
- Analysis methods that can aid the prediction of consequences on a higher system level in radio networks and for human factors are needed.

# 9 CONCLUSIONS

The results in this report clearly show that the development of the future defence requires new advanced methods to handle intersystem-interference problems. Completely new analysis methods are needed since the interference effects appear as higher-order effects on system-of-system levels and on human factors. Furthermore, it is important to consider the total ambient environment to provide reliable results of the intersystem-interference analyses for these coming systems. The underlying driving force for the development within wireless systems domains is the emerging software defined radio technologies for dynamic and flexible systems. We are here facing the problem of dynamic interference control or dynamic interference avoidance. The coming flexible and dynamic wireless solutions open up new possibilities for mobile ad hoc networks. In such networks the consequences of intersystem-interference are much more difficult to predict in advance than they are on traditional wireless links. Therefore analysis tools capable of integrating network models, wave-propagation models and intersystem-interference models must be developed. In this report we have shown examples of how such hybrid analysis models can be used.

In summary, the following conclusions are drawn from the results in this report.

- Experience shows that an increasing amount of joint and combined operations will increase the risk of future intersystem-interference problems.
- Analysis methods that can aid the prediction of consequences on a higher system level and for human factors are needed. Methods to estimate the consequences of intersystem interference in ad hoc networks must be developed.
- Intersystem interference analysis methods for on-line (on-demand) use must be developed to handle dynamic changes both in space (physical location) and time.
- Analysis methods for a reduced number of in-going system parameters must be developed.
- Intersystem interference analysis methods that include the total electromagnetic environment, e.g. ambient noise, must be developed in order to provide reliable results for the coming wireless systems.
- Emerging radio technologies such as UWB and smart antennas, increase the risks of future intersystem-interference problems.
- Emerging platform technologies such as UAV/UCAV and multi-role platforms increase the risks of future intersystem-interference problems.
- The evolution against dynamic spectrum access increases the risks of future intersystem-interference problems.
- The results show that even for low data rates and levels of interference that affect all vehicles in the mechanized battalion, there are situations where the battalion commander may not have sufficient

position information about the companies area coverage. Even if the position errors are not significant in themselves, there is a considerable variability that reduces the predictability of the positioning service.

- The position error is unacceptable for the battalion commander's information about the companies' area coverage when there is medium or high levels of interference. The unpredictability of the position error at low levels of interference may also decrease the battalion commander's trust in the SA service. Finally, there are situations where there is a potential risk for fratricide that not be excluded until a line of sight measure has been included in the analysis.

# 10 SUGGESTED TOPICS FOR FUTURE WORK

The consequences of using the "interference temperature" as model for quantifying and managing radio frequency interference should be further investigated. The interference temperature is proposed by FCC in the U.S. One problem is that the interference temperature only takes the power, not the waveform, of an interfering signal into consideration. Thus, this metric could be too blunt and must be further investigated to determine the risks of under/overestimation the interference impact if used.

In the future more and more operations are likely to take place in an urban environment, this may especially be the case for international operations. A peacekeeping mission can rapidly change into a peace enforcement mission and the ability of combat in an urban terrain can be crucial. The tactical behaviour is different in an urban terrain and the soldiers are more often dismounted than they would be in a non-urban terrain. The ability to search inside buildings is important and at the same time risky. The demands on technical systems are different and there might be specific systems for combat in an urban terrain. The ability to communicate directly between soldiers when dismounted may demand a different communication system than the system used for communication between vehicles. From a communication system point of view, the wave propagation in a city is difficult and the noise level is usually also higher in a city. This combined with the number of civilian communications systems that are working in a city makes it important to study an urban scenario in more detail, from an intersystem interference point of view.

The risk of intersystem interference when performing different kinds of electronic warfare is important to analyse. It is important to have the ability to jam the enemies communication systems without losing one's own communications, for example if a building shall be cleared it is an advantage to jam the mobile phones in the building and maintain the own communication. Analyses of intersystem interference risks due to jamming in urban environments are therefore important to perform.

Further research is required to establish how the position errors and the variability of position errors affect the operators' trust in SA services. Preferably, by asking SMEs for subjective ratings of how they experience the SA services on an appropriate scale of trust. Further results may also be obtained from the network simulations by including a line of sight measure to assess the risk for fratricide. A further analysis may also compare the battalion commander's position information with the company commander's position information for an assessment of the potential for confusion when the company commanders receive support about the location of specific vehicles. All analyses may also benefit from using distributions of time delays as the common method of comparison.

In order to jam the traffic in a communication network efficiently it is an advantage if a bottleneck in the network can be found. If the node(s) that is

crucial for the communication is jammed the damage is probably larger than if jamming is applied randomly. For intersystem interference it is the opposite case, it is extra important that the bottleneck nodes are free from intersystem interference if the network shall work properly. Methods to find these bottlenecks are important to develop for future use.

The simulations necessary to judge the effects of intersystem interference in a communication network are quite time-consuming. Hence, if it shall be possible to analyse the effects from intersystem interference in a tool simplified methods for simulating the network are necessary. Another way is to make rough estimations of the network capacity with some other method than simulations. Such methods should be investigated further to make sure that the reliability in the results are sufficient for the network analysis and moreover if it is possibly to add interference sources in the network.

The effects from other types of interference such as other legal users in an ad-hoc network are important to have knowledge about. In some cases the interference cannot be modelled as additive white Gaussian noise (AWGN) that is constant over time in the receiver. For example if a frequency hopping transmitter is interfering with the receiver in consideration the interference must be modelled differently than time constant AWGN. The analysis of this case is made on link level but the consequences in a network remain to be investigated.

# 11 APPENDIX: CALCULATION OF INTERFERENCE LEVELS

The standard EN55022 class B [38] sets limits on the maximum allowed electric field strength for computers sold within EU. For frequencies above 230 MHz the limit is 37 dBμV/m in 120 kHz bandwidth at 10 meters distance [38].

The disturbance power, $P_{\mathrm{COTS}}$ in the receiver can be estimated as [38]:

$$P_{\mathrm{COTS}} = \frac{\lambda^2}{4\pi Z_0} pqG_{\mathrm{R}} E_{\mathrm{R}}^2(r),$$

where

$\lambda$ wavelength [m]

$Z_0$ wave impedance for free space (= 377 Ω)

$p$ polarization matching factor $0<p\leq 1$

$q$ matching factor between radio antenna impedance and load impedance $0<q\leq 1$

$G_{\mathrm{R}}$ antenna gain of the receiving antenna in the direction of the disturbance

$E_{\mathrm{R}}(r)$ electrical field strength [V/m] of the disturbance at the receiver antenna

$r$ distance [m] between the disturbance source and the receiver antenna

In the equation above it is assumed that the electrical field strength is measured or specified with the same bandwidth, $W$, as the radio receiver uses. The power spectral density of the disturbance is

$$N_{\mathrm{I}} = \frac{P_{\mathrm{COTS}}}{W}.$$

We assume that the field strength decays with a factor 1/r for distances up to 10 meters and with a factor of $1/r^2$ for distances over 10 meters. In the standard the field strength was given at a distance of 10 meters and if we want the field strength at another distance, for example 3 meters. The limit for the field strength in the standard is 37 dBμV/m.

$$E_{\mathrm{R}}(3) = \frac{10 * E_{\mathrm{R}}(10)}{3} = \frac{10 * 10^{37/20} * 10^{-6}}{3}.$$

The wavelength of the disturbance is the speed of light divided by the frequency of the disturbance. The frequency is 300 MHz, which yields a wavelength of one meter. We also assume that $p$ and $q$ equals one. The bandwidth is 120 kHz and the antenna gain is assumed to be one.

$$N_{\mathrm{I}} = \frac{P_{\mathrm{COTS}}}{W} = \frac{\lambda^2}{4\pi Z_0} pqG_{\mathrm{R}} \frac{E_{\mathrm{R}}^2(3)}{W} = \frac{(c/f)^2}{4\pi Z_0} pqG_{\mathrm{R}} \frac{\left(10/3 * E_{\mathrm{R}}(10)\right)^2}{W} = 9.8 * 10^{-17} \left[\frac{W}{Hz}\right]$$

The spectral density of the noise in the receiver is denoted $N_0$ and $N_0 = kT$, where $k$ is Boltzmanns constant and $T$ is the noise temperature. We want to express the noise in terms of the noise figure $F$, defined as $F=T/T_{0,}$ the noise figure can also be expressed as $F=N_0/kT_{0,}$ where $kT_0$= -204 dBW/Hz. Without the interference present the noise figure is 10 dB. With the interference present a new noise figure can be calculated. The spectral density of the disturbance is added to the spectral density of the noise.

$$F = \frac{N_0 + N_{\mathrm{I}}}{kT_0}$$

New noise figures have been calculated for distances of 3, 10 and 20 meters. When the original noise figure is 10 dB the new noise figures are 44, 33 and 22 dB respectively.

# 12 REFERENCES

[1] Mario Lucchese, C. Leslie Golliday jr, Anil N. Joglekar, ”Operational Evaluation of Electromagnetic Environmental Effects (E3)”, Institute for Defense Analyses, PM: May – June 2000.

[2] Material from SNDC

[3] Bengt Boberg, Fredrik Eklöf, Lars Pääjärvi, ”Störning av navigeringssystem, slutrapport,” Användarrapport FOI-R--1018--SE, December 2003, in Swedish.

[4] P. Stenumgaard, “Telekonfliktforskning vid FOI 1995-2002, slutrapport,” Defence research Agency, Div. of Command and Control Systems., Linköping, Sweden, User Report FOI-R—0682—SE, December 2002, in Swedish.

[5] P. Stenumgaard, ”Utbildningskompendium Telekonflikt,” Defence research Agency, Div. of Command and Control Systems., Linköping, Sweden, Memo Dnr 01-3924 Mars 2004, in Swedish.

[6] F. Eklöf and B. Johansson, “Position distribution service for mechanised units,” Defence Research Est., Div. of Command and Control Warfare Tech. Linköping, Sweden, User Report FOA-R--00-01734-504--SE, December 2000, in Swedish.

[7] A. Hansson, J. Nilsson, M. Sköld, and U. Sterner, ”Tactical radio access networks – a comparison of cellular and ad hoc network concepts,” Defence research Agency, Div. of Command and Control Warfare Tech., Linköping, Sweden, Technical Report FOI-R--0086--SE, March 2001.

[8] P. Holm, “UTD-diffraction coefficients for higher order wedge diffracted fields,” *IEEE Trans. Antennas Propagat*., vol. AP-44, no. 6, pp. 879-888, June 1996.

[9] B. Asp, G. Eriksson, and P. Holm. “Detvag-90® -- Final Report,” Defence Research Est., Div. of Command and Control Warfare Technology, Linköping, Sweden, Scientific Report FOA-R—97-00566-504—SE, Sept. 1997.

[10] R. Raphael and S. Moshe, *Multiple Access Protocols Performance and Analysis*, Springer-Verlag, 1989.

[11] J. Grönkvist, “Assignment Strategies for Spatial Reuse TDMA,” Royal Institute of Technology, TRITA–S3-RST--0202, ISSN 1400-9137, ISRN KTH/RST/R--02/02--SE, Mars 2002.

[12] D. Young, "USAP: A unifying dynamic multichannel TDMA slot assignment protocol," in IEEE MILCOM, 1996, pp. 235-239.

[13] M. Gerla, X. Hong, and G.Pei, "Fisheye State Routing Protocol (FSR) for Ad Hoc Networks," IETF Internet Draft (work in progress), June 2002, draft-ietf-manet-fst-03.txt.

[14] K. Persson, E. Johansson, U. Sterner, and Mattias Sköld, "The Fisheye Routing Technique in Highly Mobile Ad Hoc Networks," Swedish Defence research Agency, Div. of Command and Control Systems., Linköping, Sweden, Methodology Report FOI-R--1058--SE, December 2003.

[15] Muir, B. M., & Moray, N. (1996). "Trust in automation. Part II: Experimental studies of trust and human intervention in a process control simulation," *Ergonomics*, 39, pp. 429-460.

[16] Fransson, J., Albinsson, P.-A., Stjernberger, J., & Axelsson, M. (2002*).* "Usability evaluation of FUM SLB regarding time-critical command and control," Base Data Report FOI-R--0677--SE, December 2002 (Swedish). Swedish Defence Research Institute, Linköping, Sweden.

[17] Luhman, N. (1980). *Trust and power*. New York: Wiley.

[18] Barber, B. (1983). *The logic and limits of trust*. NJ: Rutgers University Press.

[19] Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in Close Relationships*. Journal of Personality and Social Psychology*, 49(1), 95-112.

[20] Muir, B. M. (1994). "Trust in automation. Part I: Theoretical issues in the study of trust and human intervention in automated systems," *Ergonomics*, 37, pp. 1905-1922.

[21] Jian, J.-Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an Empirically Determined Scale of Trust in Automated Systems. *International Journal of Cognitive Ergonomics*, 4(1), 53-71.

[22] Muir, B. M. (1987). "Trust between humans and machines, and the design of decision aids*," International Journal of Man-Machine Studies*, 27, pp. 527-539.

[23] Lee, J., & Moray, N. (1992). "Trust, control strategies and allocation of functions in human-machine systems," *Ergonomics*, 35, pp. 1243-1270.

[24] Lee, J., & Moray, N. (1994). Trust, self-confidence, and operators' adaptation to automation. *International Journal of Human-Computer Studies*, 40, 153-184.

[25] Andersson, J., Malm, M., & Thurén, J. (2003*),* "System trust," Scientific report, FOI-R--1121--SE (in Swedish). Swedish Defence Research Establishment, Linköping, Sweden.

[26] Alvå, P., & Palmqvist, U. (2003)*,* "Battle management support systems in NCW - Scenario," Base data report, FOI-R--1030--SE (in Swedish). Swedish Defence Research Institute, Sweden.

[27] Fransson, J. (2004). Personal communication.

[28] Albinsson, P.-A., & Fransson, J. (2002). Representing military units using nested convex hulls - coping with complexity in command and control. In *Proceedings of the First Swedish-American workshop on modeling and simulation* SAWMAS-2002 (pp. 25-32). FOI-S--0672--SE. Swedish Defence Research Establishment, Linköping, Sweden.

[29] www.sdrforum.org

[30] http://jtrs.army.mil/sections/programinfo/fset_programinfo.html

[31] Rofheart,"Relax & wait", *IEE Communications Engineer*, pp 10-13, December/January 2003/04

[32] Karina Fors," Implementation of an intersystem interference model in ELSA software demonstrator", User report, FOI-R--0166--SE, Swedish Defence Research Agency, July 2001.

[33] Sara Linder, Jouni Rantakokko, Peter Stenumgaard, "A new approach for estimating the impact of electromagnetic in-band interference on digital communication systems," *Proceedings of EMC Europe 2002 International Symposium on Electromagnetic Compatibility*, Sorrento, Italy September 2002.

[34] Sara Linder, Marcus Rundgren, "Tactical consequences of intersystem interference," User report FOI-R--00-01704-504--SE, Swedish Defence Research Agency, December 2000 (in Swedish).

[35] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, as amended through December 7, 1998 (Joint Publication 1-02).

[36] G.A. Jackson," The early history of radio disturbance," *Journal of the Institution of Electronic and Radio Engineers*, no. 6, pp. 244-250, November/December 1987.

[37] Fredrik Berggren, Olav Queseth, Jens Zander, Börje Asp, Christian Jönsson, Peter Stenumgaard, Niklas Z Kviselius, Bertil Thorngren, Urban Landmark, Jonas Wessel, “Dynamic Spectrum Access - Scenarios and research challenges”, ISRN KTH/RST/R--04/07--SE September 2004.

[38] Peter F. Stenumgaard, ”A simple method to estimate the impact of different emission standards on digital radio receiver performance,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 39, pp. 365-371, November 1997.