FOI is an assignment-based authority under the Ministry of Defence. The core activities are research, method and technology development, as well as studies for the use of defence and security. The organization employs around 1350 people of whom around 950 are researchers. This makes FOI the largest research institute in Sweden. FOI provides its customers with leading expertise in a large number of fields such as security-policy studies and analyses in defence and security, assessment of different types of threats, systems for control and management of crises, protection against and management of hazardous substances, IT-security an the potential of new sensors.

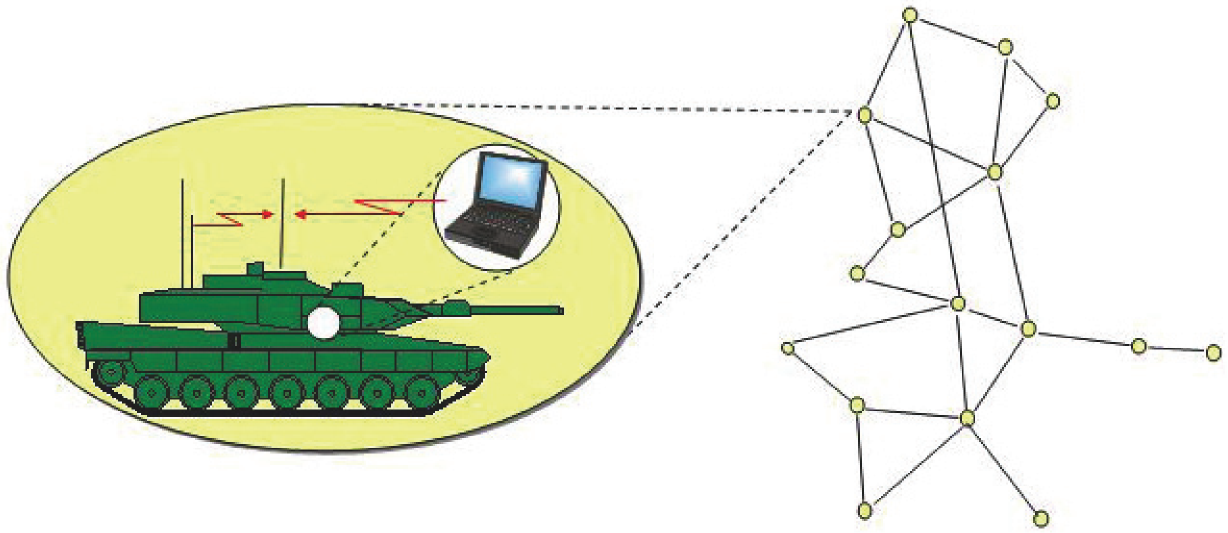
FOI
Defence Research Agency
Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping

Phone: +46 13 37 80 00
Fax: +46 13 37 81 00

www.foi.se

Methods for intersystem-interference analyses in dynamic wireless communication networks

PETER STENUMGAARD, SARA LINDER,
ULF STERNER, PETER SVENMARCK, KARINA FORS



FOI-R-- 1868 --SE Methodology report **Command and Control Systems**
ISSN 1650-1942 December 2005

Methods for intersystem-interference analyses in dynamic wireless communication networks

FOI-R----SE
ISSN 1650-1942

Command and Control Systems
Methodology report

December 2005

<table>
<tr><td rowspan="5">Issuing organization
FOI – Swedish Defence Research Agency
Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping</td><td>Report number, ISRN
FOI-R--1868--SE</td><td>Report type
Methodology report</td></tr>
<tr><td colspan="2">Research area code
4. C4ISTAR</td></tr>
<tr><td>Month year
December 2005</td><td>Project no.
E7956</td></tr>
<tr><td colspan="2">Sub area code
41 C4I</td></tr>
<tr><td colspan="2">Sub area code 2</td></tr>
<tr><td rowspan="4">Author/s (editor/s)
Peter Stenumgaard
Sara Linder
Ulf Sterner
Peter Svenmarck
Karina Fors</td><td colspan="2">Project manager
Peter Stenumgaard</td></tr>
<tr><td colspan="2">Approved by
Sören Eriksson</td></tr>
<tr><td colspan="2">Sponsoring agency
Swedish Defence Materiel Administration (FMV)</td></tr>
<tr><td colspan="2">Scientifically and technically responsible
Jan Nilsson</td></tr>
<tr><td colspan="3">Report title
Methods for intersystem-interference analyses in dynamic wireless communication networks</td></tr>
</table>

Abstract

The Swedish Defence has a need of developing new analysis methods for intersystem interference. FOI performs a number of research activities in order to support this development by ensuring that new dynamic communication systems can be handled in a future analysis tool. A key issue is the ability to consider the total electromagnetic-interference environment within the receiver band of a wireless communication system. Furthermore, to determine what consequences intersystem interference could have on the network level of a wireless communication network.

The method based on only using the total average interference power is investigated to see if the uncertainties connected with this method are small enough when conclusions on the network level in an ad hoc network are to be drawn. Furthermore, the commercial network analysis tool OPNET Modeler is investigated to see if that tool is a convenient software environment for a new analysis tool. Finally it is investigated how an operators´trust could be affected by intersystem interference in a communication network.

The results show that the total average power is useful if a proposed correction factor is used to eliminate the largets uncertainties. It is also shown that OPNET Modeler is a possible candidate as a basic software environment for a future intersystem-interference analysis tool for defence applications. It is also shown that intersystem interference, in some cases, severely can affect a commanders´situation awareness and trust.

Keywords

Intersystem interference, wireless communication, pulsed interference, ad hoc networks

Further bibliographic information	**Language** English
ISSN 1650-1942	**Pages** 58 p.
	Price acc. to pricelist

Utgivare FOI - Totalförsvarets forskningsinstitut Ledningssystem Box 1165 581 11 Linköping	**Rapportnummer, ISRN** FOI-R--1868--SE	**Klassificering** Metodrapport
	Forskningsområde 4. Ledning, informationsteknik och sensorer	
	Månad, år December 2005	**Projektnummer** E7956
	Delområde 41 Ledning med samband och telekom och IT-system	
	Delområde 2	
Författare/redaktör Peter Stenumgaard Sara Linder Ulf Sterner Peter Svenmarck Karina Fors	**Projektledare** Peter Stenumgaard	
	Godkänd av Sören Eriksson	
	Uppdragsgivare/kundbeteckning Försvarets Materielverk (FMV)	
	Tekniskt och/eller vetenskapligt ansvarig Jan Nilsson	

Rapportens titel

Metoder för telekonfliktanalyser i dynamiska trådlösa kommunikationssystem

Sammanfattning

Försvarsmakten har behov av att utveckla helt nya analysmetoder för telekonflikter. FOI utför ett antal forskningsuppgifter som direkt stödjer denna utveckling för att tillgodose att nya dynamiska kommunikationssystem kan hanteras i ett framtida analysverktyg. En nyckeluppgift är förmågan att ta hänsyn till den totala elektromagnetiska störningsmiljön i mottagarbandet hos ett trådlöst kommunikationssystem samt att kunna påvisa vilka effekter en telekonflikt kan få på nätnivå i ett trådlöst kommunikationsnät.

Metoden att endast använda den totala medeleffekten hos en störning undersöks i denna rapport för att avgöra om de osäkerheter som är förknippade med metoden är tillräckligt låga för att dra slutsatser på nätnivå i ett trådlöst kommunikationsnät av ad hoc-typ. Vidare undersöks om det kommersiellt tillgängliga verktyget för nätanalys; OPNET Modeler, är en lämplig verktygsmiljö för det kommande telekonfliktverktyget. Slutligen undersöks hur en operatörs systemtilltro kan påverkas av telekonflikter i ett kommunikationsnät.

Resultaten visar att den totala medeleffekten är användbar om en föreslagen korrektionsfaktor används för att eliminera de största osäkerheterna. Det visas även att OPNET Modeler är en möjlig kandidat som grundmiljö för ett datorbaserat verktyg för telekonfliktanalyser i försvarstillämpningar. Resultaten visar också att telekonflikter allvarligt kan påverka en förbandschefs lägesbild och systemtilltro.

Nyckelord

Telekonflikt, interferenser, trådlös kommunikation, pulsad störning, ad hoc nät

Övriga bibliografiska uppgifter	**Språk** Engelska
ISSN 1650-1942	**Antal sidor:** 58 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Content

1 Background

1.1 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. 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 [16]. Hence, the problem of intersystem interference is now more important to handle than ever. Existing state-of-the-art analysis methods for intersystem interference in wireless services are often 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 [16]. Furthermore, existing methods are focused on the single transmission/ receiver link level. 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). One drawback with this simplified approach is that the waveform of an interference signal can dramatically affects the impact on a digital system. Unfortunately, for some interference signals, this approach significantly underestimates the impact on a digital communication system [4]. 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 Fig. 1.1. 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. Typically,

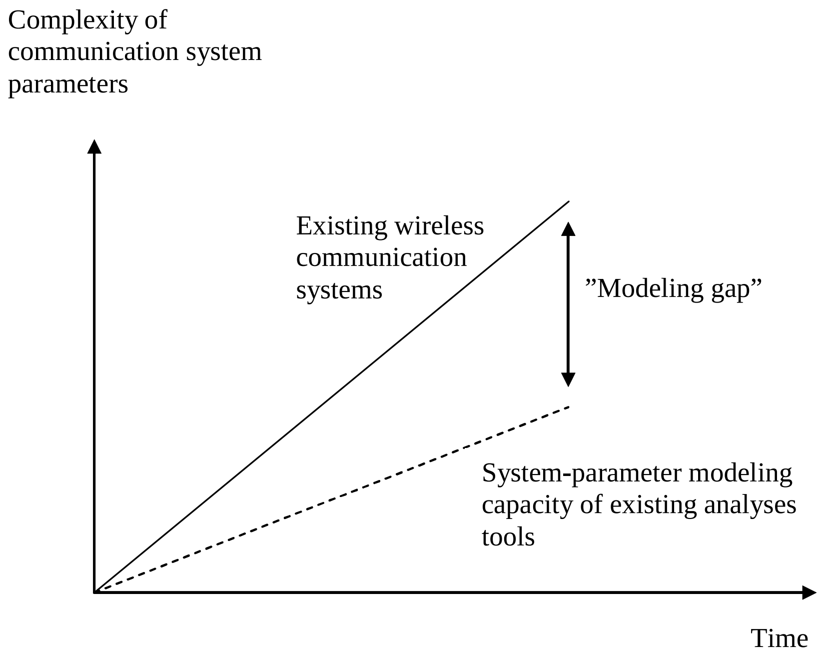


Figure 1.1: A schematic view showing that the capacity to handle the increasing amount of system parameters is to low in existing analysis tools for intersystem interference.

the final result is obtained by worst-case assumptions where the simultaneous impact from different interference sources is considered. This means a situation that is statistically unlikely to occur. In summary, the current situation of traditional intersystem-interference analysis tools is that

- 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 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.

In a dynamic network scenario, the intersystem-interference analyses cannot be performed in advance for a limited number of static cases. This is because the number of potential intersystem-interference cases will be too large, almost infinite. Furthermore, the necessary intersystem-interference analyses must include the total actual interference environment, i.e. not only the known intentional/unintentional transmitters. The intersystem-interference analyses must be done on line for each case. This means that all kinds of background interference will affect the result of these analyses for a certain system. Since the analyses must be done on line, no detailed information, such as system specification parameters, of the actual interference signal will be available. The analyses will be based on some kind of more or less simple measured value of the total interference at the moment. Thus, reliable analysis methods based on a reduced number of interference-signal parameters must be available. Consequently, several major evolutions of present analysis methods for intersystem interference are needed:

- 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 and for human factors are needed.

One parameter proposed is the so called “interference temperature” which has been proposed by the Federal Communications Commission (FCC) [2]. The interference temperature is simply a measurement of the total RF power generated by undesired emitters plus noise sources that are present in a receiver system per unit bandwidth. More specifically, it is the temperature equivalent of this power measured in units of “Kelvin” (K). One difficulty with such approach is that the interference impact on modern digital communication systems from an interference signal does not only depend on the power but also on the actual waveform of the interference signal. Thus, only using the power of an interference signal to determine the impact on a digital communication system, can give large errors in terms of interference impact. In this report we investigate the interference-temperature concept to see if it is useful in a future computer-based tool for intersystem-interference analyses. We propose a quality measure of the interference temperature approach which makes it possible to adjust for the interference-waveform properties so that the measured total interference power can be used as the desired decision metric in future applications. This opens the possibility to use simplified models of the intersystem interference when the consequences on dynamic wireless networks are to be determined.

1.2 Scope

This report summarizes the work performed in order FMV 281273-LB673859, 2005-05-03, issued by Leif Junholm at the Swedish Defence Materiel Administration, Center of Expertise in Sensors & Telecommunications. The work performed within this order is a continuation of the work presented in [16]. The overall purpose with the different subtasks in this order is to provide further knowledge useful for the development of a new computer-based tool for intersystem-interference analyses. These subtasks represent a selected amount of important questions that have to be answered to support the coming specification work of the new analysis tool.

1.3 Outline

In chapter 2, the so called Interference Temperature concept is evaluated on a communication link level. It is shown that for pulsed interference, a correction factor is convenient to use in order to decrease the errors introduced if only the interference-signal power is used as input to a Gaussian approximation. In chapter 3, it is investigated how the errors introduced on link level affects the results at the network level for a situation awareness service. In chapter 4, the impact of intersystem interference on trust in a situation-awareness service is investigated. It is shown that intersystem interference can have large impact on the operators trust in certain situations. In chapter 5, the possibility to use OPNET Modeler as a basis for a new intersystem-interference analysis tool is investigated and it is concluded that this is possible if simplified models of the intersystem interference on platforms can be used. In chapter 6, the publications within the project are listed. The conclusions are summarized in chapter 7 and suggestions for further work are given in chapter 8.

2 Interference Temperature and link analyses

2.1 Background

The emerging Software Defined Radio technologies will be an enabler for a new generation of dynamic flexible wireless systems. It will also open up the possibility of allocating frequencies in a more dynamic way than today. From an EMC point of view this can cause unforeseen interference problems to occur due to the increased complexity in such future applications. In a dynamic spectrum allocation context, a measure indicating whether or not a frequency band is possible to use from an electromagnetic interference point of view, must be found. The Federal Communications Commission (FCC) has proposed a measurement of the total interference power within the receiver band, expressed as noise temperature (interference temperature), as a practical decision metric for this problem. One difficulty with such approach is that the interference impact on modern digital communication systems from an interference signal does not only depend on the power but also on the actual waveform of the interference signal. Thus, only using the power of an interference signal to determine the impact on a digital communication system, can give large errors in terms of interference impact. In this report, however, we introduce a quality measure of the interference temperature approach which makes it possible to adjust for the interference-waveform properties so that the measured total interference power can be used as the desired decision metric in future applications.

2.2 Introduction

The background of the Electromagnetic Compatibility (EMC) area 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 electrical noise and similar man-made 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 (CISPR). The International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) were cofounders [1]. 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 CISPR. Since then, the EMC area has however been undergone tremendous growth with the birth of a large amount of sub areas. Today the EMC area is a well-established engineering and scientific domain all over the world. However, current emission standards and interference-avoidance policies are still based on knowledge and principles of the impact on analog services from electromagnetic interference. In the near future it is highly probable that radio interference issues once again will lead to a rapid evolution of some research domains within the area of EMC. One such domain is closely related to the on-going development of dynamic flexible wireless networks, or software defined radios (SDR) based on software communication architectures. SDR is a key element in the design of future wireless networks providing a lot higher level of flexibility than today. One development path within SDR is Cognitive Radios (CR). Cognitive Radios are “smart” radios that easily adapt to their operating environment, seizing spectrum bandwidth whenever it becomes available.

Existing methods for intersystem-interference analyses are focused on single wireless transmission/receiver links but in the future methods to predict and analyse effects on higher levels in the networks and systems are needed. Furthermore, methods to perform some of these analyses on line in dynamic flexible wireless systems must be developed. We are here facing the problem of dynamic interference control or dynamic interference avoidance. A key issue in future dynamic and flexible wireless applications is the ability to consider the total electromagnetic interference within the receiver band of the wireless communication system. Methods considering the total interference environment must be developed for instance in order to allocate frequency spectrum dynamically on demand. The Federal Communications Commission (FCC) has initiated activities to examine a more quantitative approach to spectrum management with the goals of providing radio service licensees with greater certainty regarding the maximum permissible interference present in the frequency bands in which they operate. Furthermore, possibly allowing more opportunistic access to the spectrum by unlicensed devices. The FCC has released a Notice of Inquiry and Notice of Proposed Rulemaking [2] 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 Radio Frequency (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 pre-set limit. One difficulty with such approach is that the wave form, not only the power, of an interfering signal can significantly affect the performance of a disturbed system. This is a well-known result in earlier intersystem-interference research.

In this report, however, we introduce a quality measure of the interference temperature approach which makes it possible to adjust for the interference-waveform properties so that the measured total interference power can be used as the desired decision metric in future applications. We show that it is possible to relate the Impulsiveness Ratio, of an interference signal, to the error introduced only using the total interference power in performance estimations on digital communication systems. An Impulsiveness Correction Factor (ICF) is introduced and proposed as a quality measure for the approximate method of the interference temperature. It is shown that with this ICF it is possible to use the total interference power as a decision metric and correct for the performance errors introduced.

2.3 Digital Communication systems and pulsed interference

The performance of a digital communication system subjected to periodic pulsed interference is analyzed in [5] for pulses with a pulse width less than the symbol time of the digital communication system. In Fig. 2.1 the BEP as a function of the signal-to interference ratio (SIR) is shown for different pulse repetition frequencies (R_S is the symbol rate of the digital communication system). The modulation scheme in Fig. 2.1 is Binary Phase Shift Keying (BPSK). The SIR is the ratio of the symbol power and the interference power within the bandwidth of the digital communication receiver. The signal-to noise ratio (thermal receiver noise) is 12 dB in this figure. The BEP for the pulsed interference is compared to the BEP for Gaussian noise (Additive White Gaussian Noise, AWGN). The modulation scheme in Fig. 2.1 is Binary Phase Shift Keying (BPSK) The SIR is the ratio of the symbol power and the interference power within the bandwidth of the digital communication receiver. The signal-to noise ratio (thermal receiver noise) is 12 dB in this figure. The BEP for the pulsed interference is compared to the BEP for Gaussian noise (Additive White Gaussian Noise, AWGN). As seen, the BEP for pulsed interference differs from the BEP caused by the AWGN. However, the largest difference in SIR for a constant BEP is 7.5 dB for a shift in pulse repetition frequency f_p with one decade. The analytical proof for this is shown in [2]. In [5] it is also shown that this behaviour is true even for other digital modulation schemes. From Figure 2.1 it is obvious that only using the interference power to predict the

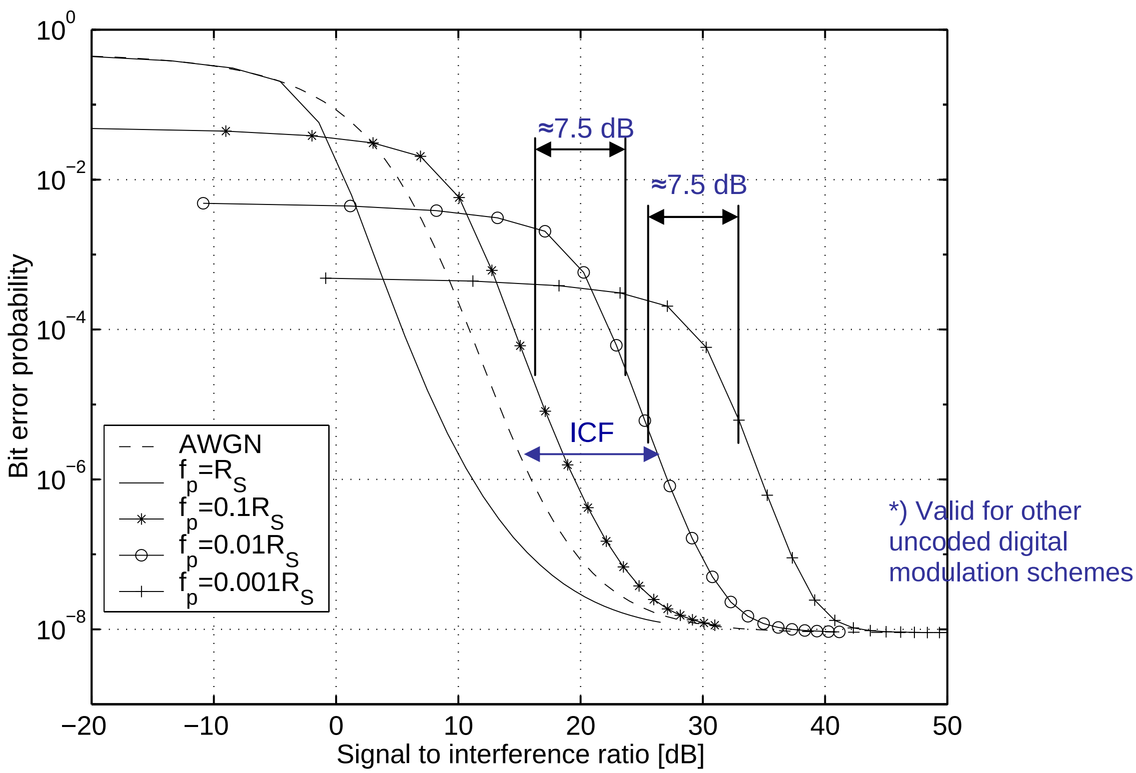


Figure.2.1: Pulsed sine wave versus Gaussian (AWGN) interference on digital communication systems if the disturbance-pulse width < symbol time of the communication system.

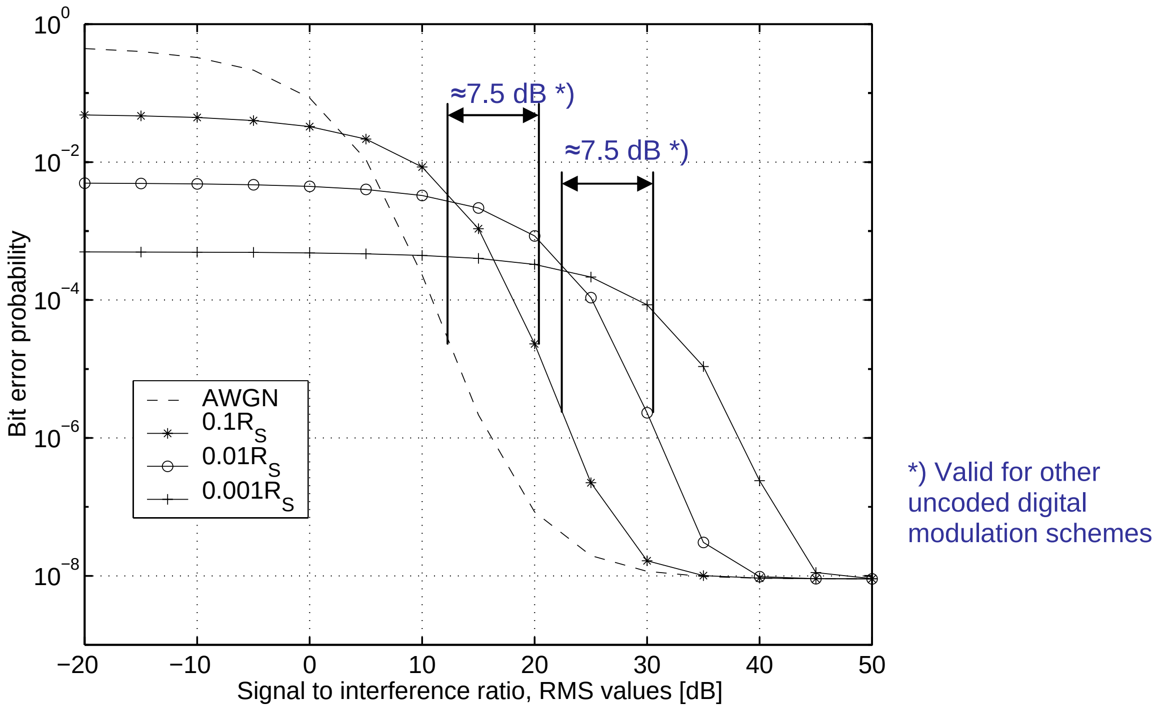


Figure. 2.2: Pulsed Gaussian (AWGN) interference on digital communication systems if the disturbance pulse width > symbol time of the communication system.

impact on a digital communication system can give large errors since the impact is strongly dependent on the waveform properties of the interference signal. These errors can be in the order of several magnitudes or up to a factor 10000 with respect to estimated BEP. If the pulse duration is greater than the symbol time of the digital communication system, the expression for the bit error probability is considerably easier to derive since we can model the situation as a two-state model where one state is when the interference pulse is present and one state is when we only have thermal receiver noise present. The bit error probability P_b for BPSK will be

$$P_b = \frac{f_p}{2R_S} erfc\left(\sqrt{\frac{E_b}{N_0 + N_I}}\right) + (1 - \frac{f_p}{R_S})\frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_0}}\right), \tag{2.1}$$

where E_b is the energy per data bit and N_0 is the single-sided power spectral density [W/Hz] of the internal noise level in the receiver. As seen in Figure. 2.2, equation (1) will also give a 7.5 dB shift when the pulse repetition frequency is shifted one decade. The difference for pulse widths > symbol time is that the BEP curves for the different pulse repetition frequencies are horizontally shifted a few dB compared to the curves for smaller pulse widths.

2.4 The impulsiveness correction factor (ICF) for pulsed interference

A well-known measure of the impulsive properties of noise is the Impulsiveness Ratio (IR) [6]. The impulsiveness ratio *IR* is defined as

$$IR = 20\log\frac{V_{\mathrm{RMS}}}{V_{average}}, \qquad \text{[dB]} \qquad (2.2)$$

where V_{RMS} and V_{average} are the root-mean square and time average values of the envelope of the output of the IF (Intermediate Frequency) filter of a measurement receiver. For periodic pulses with pulse repetition frequency f_p passed through an IF-filter with bandwidth W_{IF}, the *IR* is [19]

$$IR = 20\log\frac{\sqrt{W_{\mathrm{IF}}}}{\sqrt{f_{\mathrm{p}}}}. \qquad \text{[dB]} \qquad (2.3)$$

By inspection of Figure 2.1, the *ICF* can approximately be expressed as

$$ICF \approx \begin{cases} -4-7.5\log\dfrac{f_{\mathrm{p}}}{R_{\mathrm{S}}} & f_{\mathrm{p}} < R_{\mathrm{S}} \\ -4 & f_{\mathrm{p}} \geq R_{\mathrm{S}} \end{cases} \quad \text{[dB]} \qquad (2.4)$$

By using the common approximation $W_{\mathrm{IF}} \cong R_{\mathrm{S}}$ we can combine equation (2.3) and (2.4) so that

$$ICF \approx -4 + \frac{3}{4}IR, \qquad \text{[dB]} \qquad (2.5)$$

Thus, by knowing the Impulsiveness Ratio we can determine how much, in terms of SIR, the measured interference signal differs from a Gaussian distributed signal causing the same bit error probability at the victim, see Figure. 2.3. It should be noted that the interference power measurements should be done with the same bandwidth as the digital communication system of interest. Applying Equation (2.5) even for pulse widths > symbol time will introduce an error in SIR in the magnitude of a few dB. However, if one are looking for a simple rough correction this will reduce the error in BEP from several magnitudes to about one magnitude, despite this error in SIR. Thus, even in this case a considerable improvement is gained.

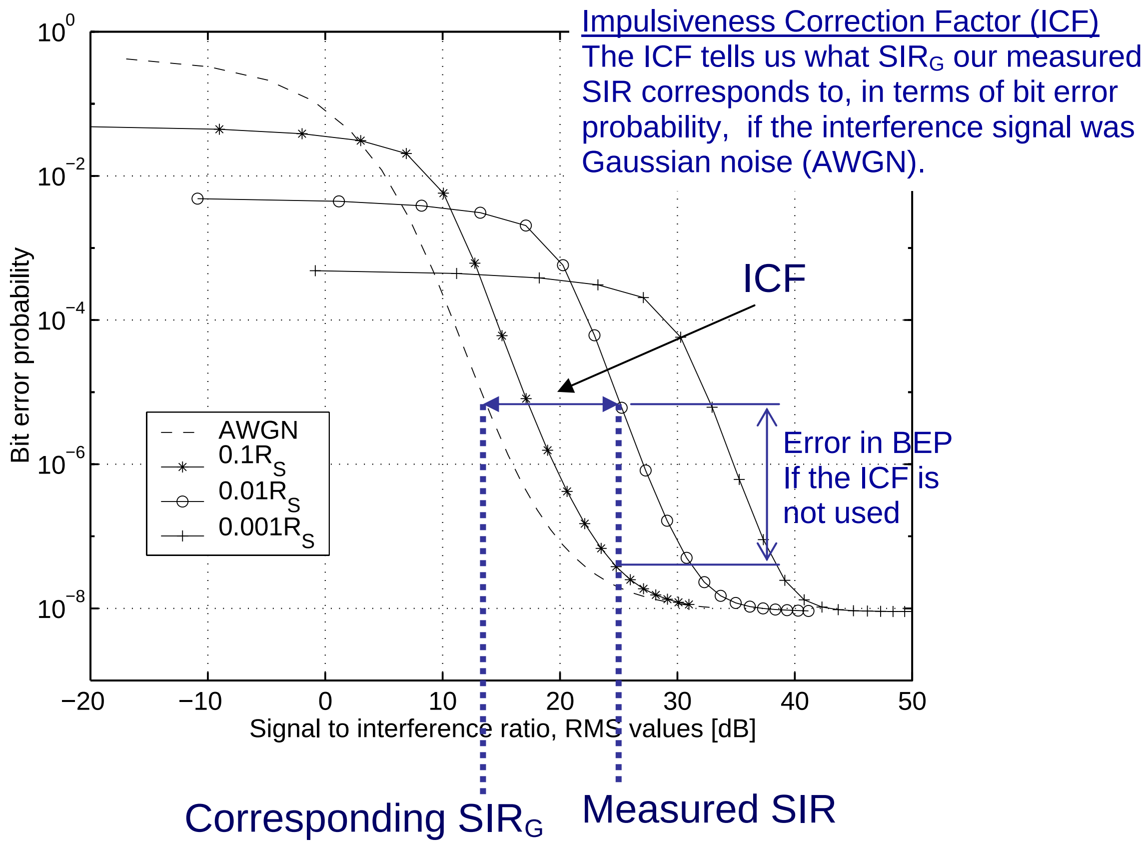


Figure 2.3: How the ICF can be used to adjust the interference temperature measurement to the corresponding value for a Gaussian noise interference signal.

2.5 Digital Communication systems and mixed interference signals

The performance of a digital receiver has been investigated for different types of interference signals. The communication system use binary phase shift keying (BPSK) and the interfering signals are pulsed signals, modulated signals or a mix of these. Simulations have been performed in Matlab. To limit the simulation time the simulations are aborted when a bit error rate of about 10^{-6} is reached. All signals are simulated with 10 samples per bit time. The signal to noise ratio (SNR) is 12 dB.

In Figure 2.4 the bit error probability (BEP) from simulations with different kinds of pulsed signals is shown. Three different kinds of pulsed interfering signals are simulated; a signal with periodic pulses and positive real amplitude, a periodic pulse with random phase and a pulse with random arrival time and random phase. All the pulsed signals have a pulse duration, T_p, of 10 % of the bit time, T_b. The periodic pulses in the figure have a pulse repetition time, T_r, of 100 times the bit time, whereas the pulsed signal with random arrival times is modeled as a Poisson process with rate $1/T_r$. In the case of pulses with random arrival time the pulses can overlap each other. In Figure 2.7 the pulses with real amplitude yield the highest BEP since they are assumed to have the same phase as the communication signal.

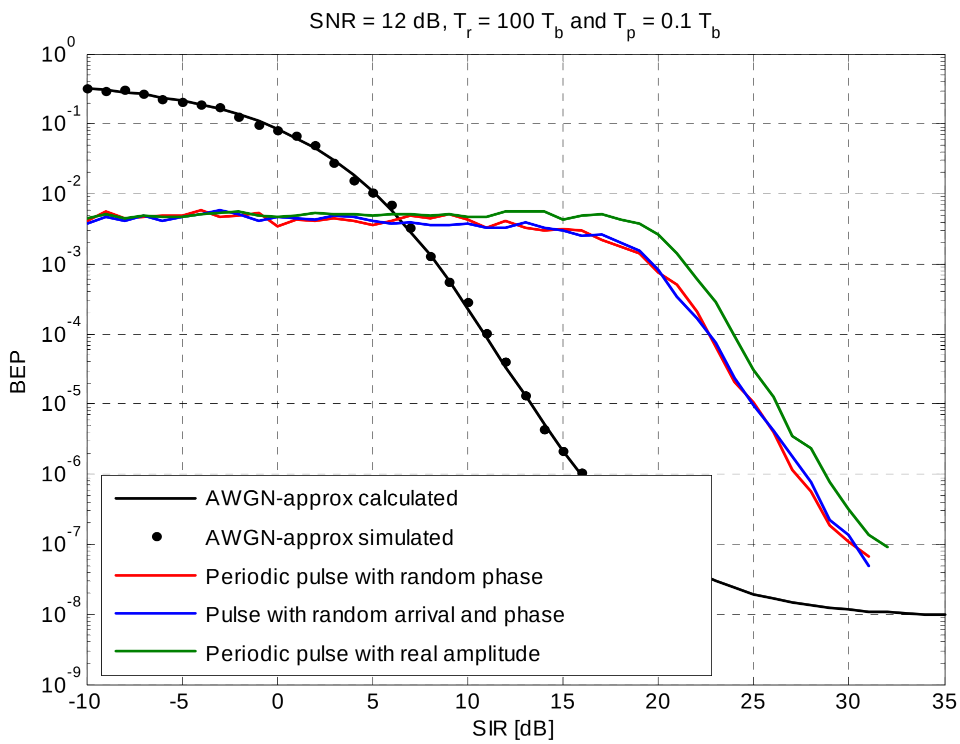


Figure 2.4: BEP for different kinds of pulsed signals.

In Figure 2.5 the impact of pulses with different pulse repetition times are shown. The results from the simulations are comparable with the analytical curves in Figure 2.1. The simulated pulses have random arrival time and a random phase. For low SIR values the BEP reaches a maximum that depends on the pulse repetition time for the pulsed signal, i.e. when a pulse is present in a bit the probability of an error is ½ and the maximum BEP is hence given by $½/T_r$ (valid if the pulse duration is shorter than the bit time). This behaviour can be seen in Figure 2.5 as different plateaus for the maximum BEP depending on the different pulse repetition times. For high SIR values the BEP depends only on the SNR value and hence only on the noise and the type of interference does not matter.

When approximating the pulsed signal the most important region is when the interference is not so strong that it yields the maximum BEP but still have an influence on the BEP. In Figure 2.5 it can be seen that using the AWGN approximation for a pulsed signal, when the BEP from the AWGN approximation is lower than the maximum BEP for the pulsed signal, yields an underestimation of the BEP. The size of the underestimation depends on the pulse repetition time of the pulsed signal and the largest difference in BEP performance from the AWGN-approximation is for the pulse with the largest pulse repetition time. The impact of an interfering BPSK modulated signal is also shown in Figure 2.5 as a reference. The BPSK modulated interfering signal is assumed to not be in phase with the communication system and hence have complex amplitude. The BEP for the BPSK signal is overestimated by the AWGN approximation if SIR is over 0 dB.

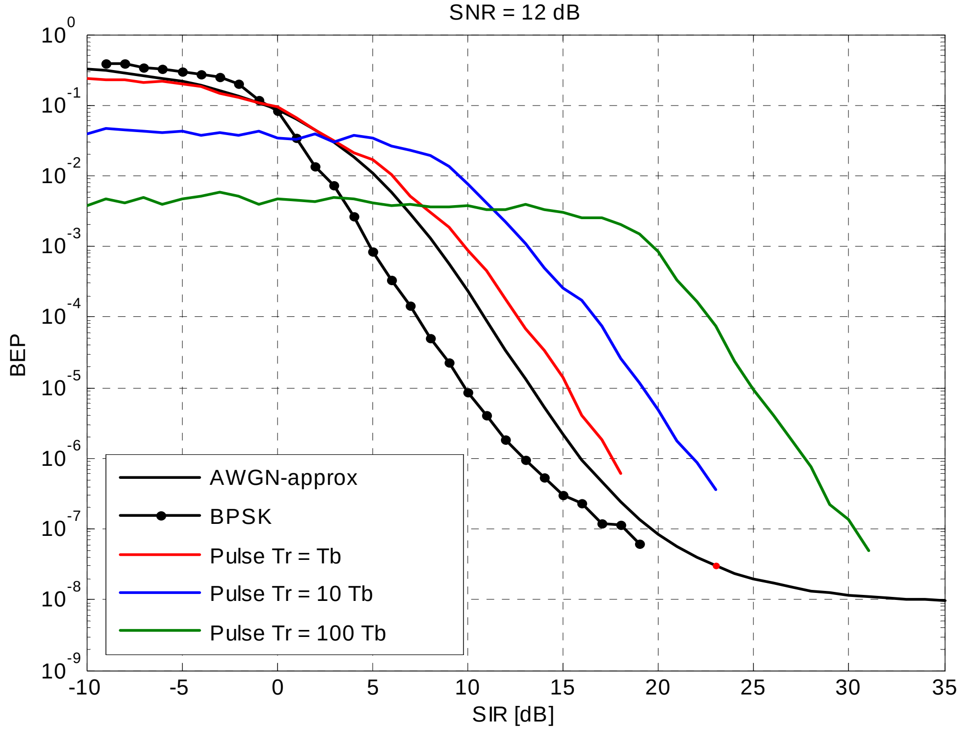


Figure 2.5: Bit error rate for different kinds of interfering signals.

Signals that consist of a number of pulsed signals have also been simulated. The power of the interference is equally divided between a number of independent pulsed signals. The interfering signals are pulsed signals with random arrival time according to a Poisson process with rate $1/T_r$. All the combined signals have the same pulse repetition times, $T_r = 100 \cdot T_b$. The BEP performance is shown in Figure 2.6.

In Figure 2.6 it can be seen that the biggest risk of underestimating the BEP with the AWGN approximation is for the case when only one pulsed signal is present. The BEP curves differ the most from the AWGN performance for the cases with few interfering signals that share the energy. When the interfering signal constitutes of many pulsed signals the BEP performance is more like the performance from AWGN.

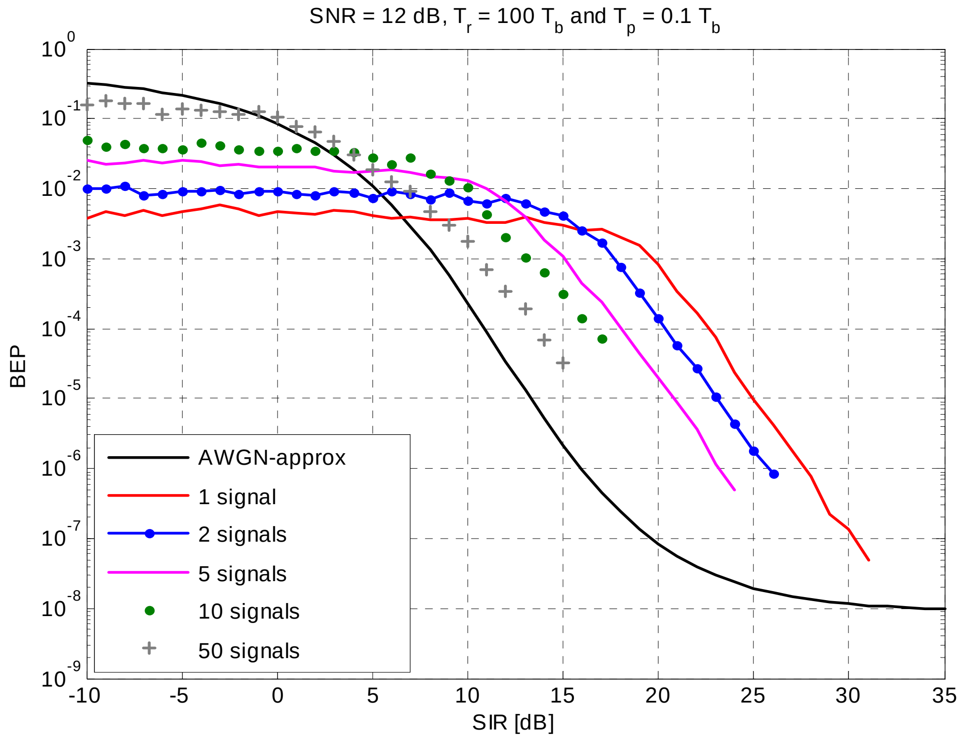


Figure 2.6: BEP for signals consisting of a different number of pulsed signals.

A mixed signal consisting of a BPSK signal and a pulsed signal is also investigated. The effects of the distribution of the total signal energy are investigated, i.e. the both signals have the same energy (half of the total each), the BPSK signal have ¾ or ¼ of the total energy.

In Figure 2.7 the BEP for different interfering signals is shown. The BEP performance is shown for an interfering BPSK modulated signal and a pulsed signal with a pulse duration that is 10% of the bit time and a pulse repetition time of 100 times the bit time. In the figure the performances for the mixed interfering signals are also shown. The pulsed signal have a BEP behavior that differs most from the AWGN approximation. When the BPSK part of the mixed signal is ¼ the performance differs only slightly from the pulsed signal except for low SIR values. When the BPSK part of the mixed signal increases the BEP curve gets closer to the performance from AWGN. This is in accordance with that the BEP from an interfering BPSK signal is lower than the BEP from an interfering pulsed signal for the same SIR for intermediate SIR values. For low SIR the resulting BEP is higher for an interfering BPSK signal than for a pulsed signal. This effect can also be seen in Figure 2.7 for low SIR values where the BEP performance is dominated by the BPSK part of the signal. However, for intermediate SIR the pulsed signal have a large impact on the BEP performance even when the BPSK part of the signal is ¾.

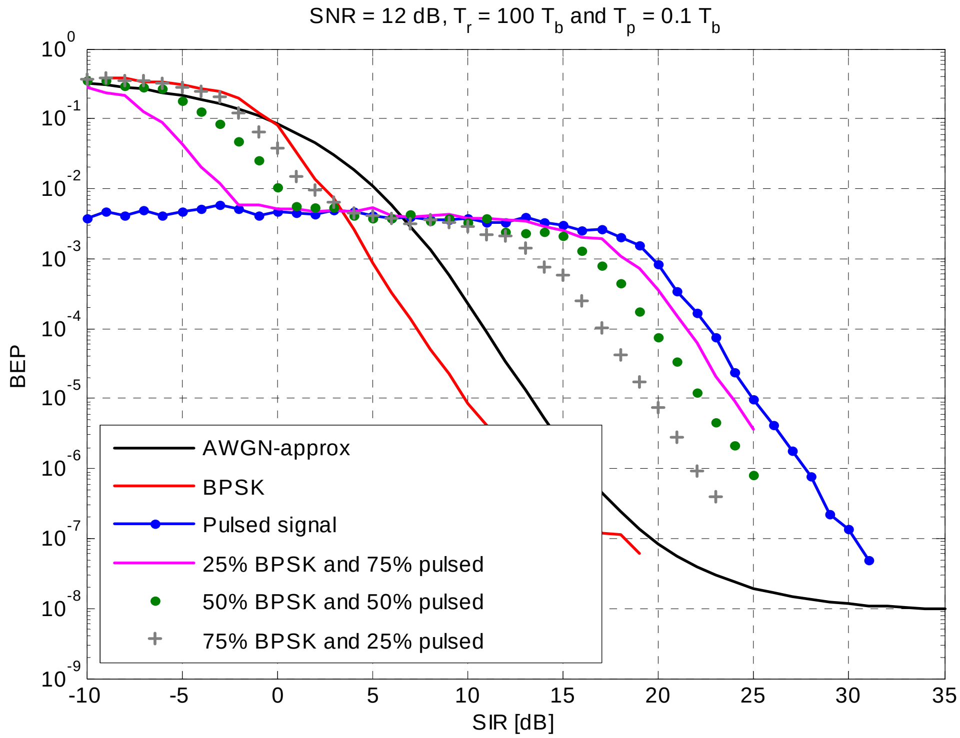


Figure 2.7: BEP for signals mixed of a pulsed signal and a BPSK modulated signal.

2.6 The impulsiveness correction factor (ICF) for mixed interference

In this section the use of the impulse correction factor (ICF) for different types of interference is investigated. The impulsiveness ratio (IR) can be calculated with equation 2.3 for a pulsed signal and the corresponding ICF can be calculated with equation 2.4. These calculated values for the pulsed signal are hereafter referred to as theoretical values. The IR and ICF can also be estimated from signals according to equations 2.2 and 2.5. From the BER curves for different types of signals a "desired" ICF value can be determined, see for example the ICF in Figure 2.3.

The ICF for a signal can be estimated using the average- and RMS-value of the signal using equation 2.2 and 2.5. The ICF is estimated in the receiver after the signal is integrated over a bit time. The ICF where estimated for sequences of length 100 000 bits and with 10 samples per bit.

The IR and ICF values for different types of pulsed signals are shown in Table 2.1. The theoretical values are calculated from equations 2.3 and 2.4. The estimated values for the both types of periodic pulses, with positive real amplitude or random phase, show a very good agreement with the theoretical values. When the arrival of the pulse is random the estimates of the IR and ICF have a larger variance but show a good agreement with the theoretical values, especially for the cases with large pulse repetition time.

Table 2.1: Theoretical and estimated IR and ICF values for different pulsed signals.

T_r/T_b	Theory		Periodic pulse				Random arrival time	
			Random phase		Positive real amplitude		Random phase	
	IR (dB)	ICF (dB)	IR (dB)	ICF (dB)	IR (dB)	ICF (dB)	IR (dB)	ICF (dB)
1	0	-4	0.00	-4.00	0.00	-4.00	2.68	-1.99
10	10	3.5	10.00	3.50	10.00	3.50	10.34	3.76
100	20	11	20.00	11.00	20.00	11.00	20.26	11.19

The ICF can have negative values but should not be used in these cases, since there is seldom a need for correcting the SIR value for the AWGN-approximation to a higher value. Hence, the ICF of -4 for the pulsed signal with $T_r = T_b$ should not be used as a correction; compare with the BEP curve in Figure 2.5 where the desired correction is about +2 dB.

In Table 2.2 the IR and ICF values are given for signals consisting of many pulsed signals. The pulsed signals have random phase and random arrival time. The ICF is plotted as a function of the number of pulsed signals in Figure 2.11. The ICF values are higher for signals consisting of pulses with long pulse repetition time. The ICF is lower for signals consisting of many pulses and the decrease is quite large when comparing the ICF for one pulsed signal with a signal consisting of 10 pulsed signals. From the BEP plot in Figure 2.6 desirable ICF values are estimated and plotted as dots in Figure 2.11. When the number of pulses is large the difference between the desired and actual ICF-value is to large for the use of the approximation. However, for the case with many interfering signals the need for an approximation is smaller since the BEP curve is more AWGN-like, see Figure 2.9. When the number of interferences is small the ICF is a good correction factor.

Table 2.2: Estimated IR and ICF values for signals consisting of a different number of pulsed signals.

T_r/T_b	2 pulses		5 pulses		10 pulses		50 pulses	
	IR (dB)	ICF (dB)	IR (dB)	ICF (dB)	IR (dB)	ICF (dB)	IR (dB)	ICF (dB)
1	1.64	-2.77	1.18	-3.11	1.10	-3.17	1.06	-3.21
10	7.59	1.69	4.47	-0.65	2.69	-1.98	1.19	-3.11
100	17.04	8.78	13.11	5.84	10.36	3.77	4.46	-0.65

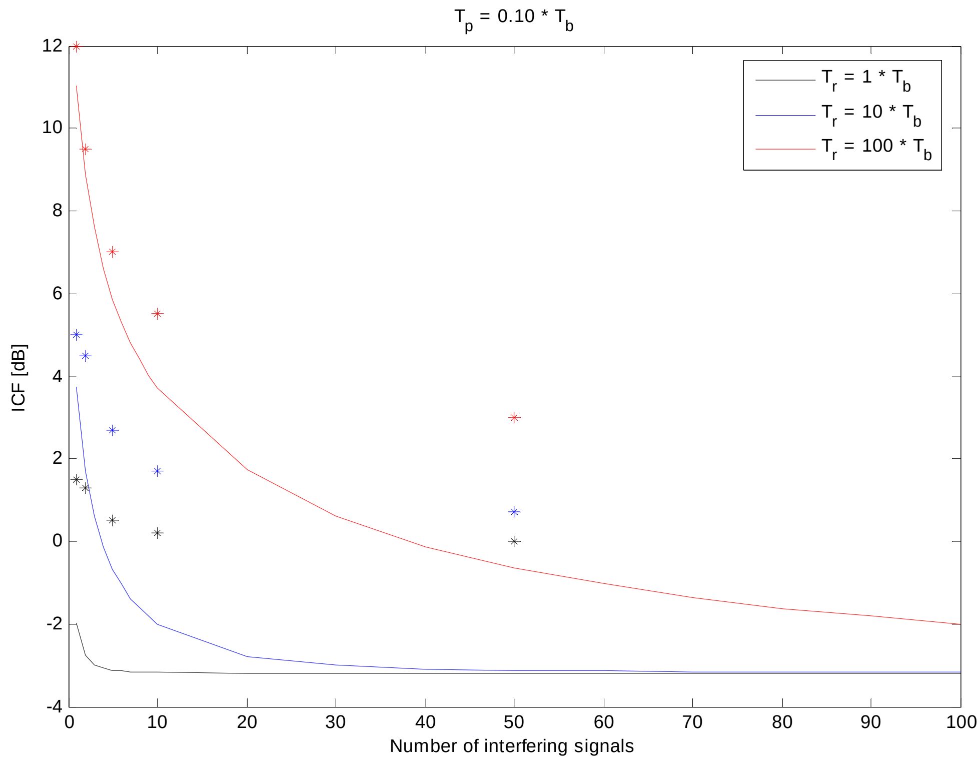


Figure 2.8: ICF as a function of number of pulsed signals with random phase and arrival time.

ICF-values estimated from signals consisting of a BPSK-signal and a pulsed signal are given in Table 2.3. When comparing the ICF-values here with the ICF values for signals containing one pulsed signal it is clear that the BPSK part have a large influence on the ICF measure even when the BPSK part of the signal is quite small. This can also be seen in Figure 2.9 where the ICF is shown as a function of the BPSK part of the mixed signal. When the value on the x-axis is zero the signal only consist of a pulsed signal and when the value is one the signal is a BPSK modulated signal. The curves represent different pulse repetition times for the pulsed part of the signal. The ICF decrease rapidly when the BPSK part is increasing from 0. Desired correction factors estimated from Figure 2.7 are shown as stars in the figure together with similar results from simulations with other pulse repetition times not shown in this report. The difference between the desired values and estimated is large for the mixed signals.

Table 2.3: Estimated IR and ICF values for signals mixed of a pulsed signal and a BPSK modulated signal.

T_r/T_b	25 % BPSK		50 % BPSK		75 % BPSK	
	IR (dB)	**ICF (dB)**	**IR (dB)**	**ICF (dB)**	**IR (dB)**	**ICF (dB)**
1	1.21	-3.09	0.90	-3.32	0.50	-3.63
10	2.87	-1.85	1.30	-3.03	0.47	-3.65
100	4.69	-0.48	2.24	-2.32	0.84	-3.37

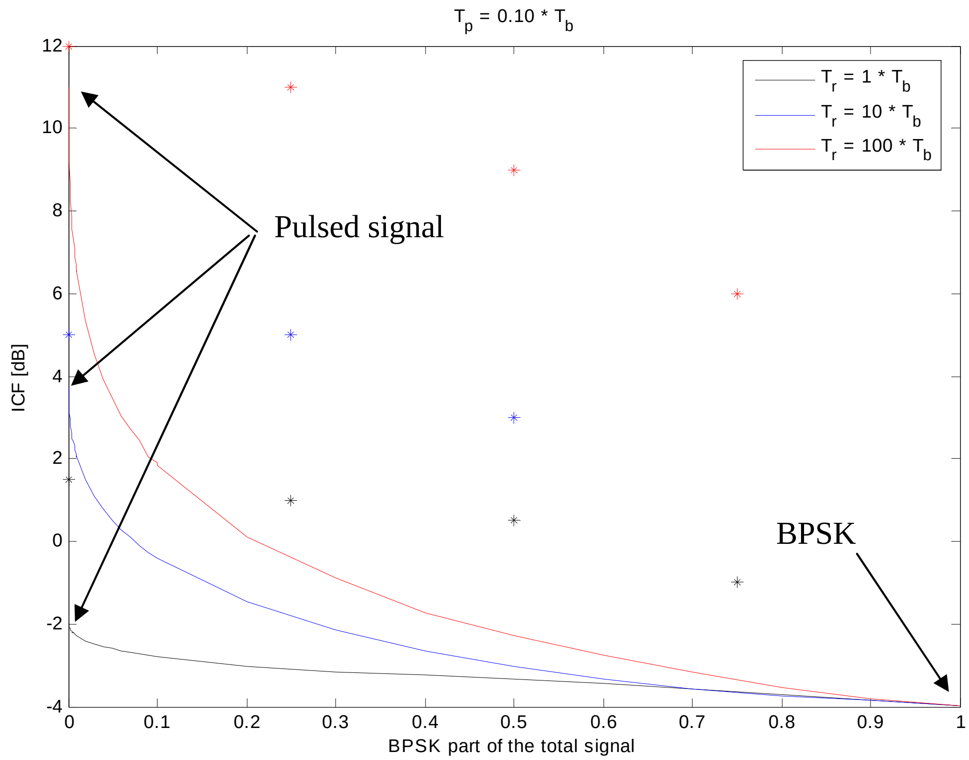


Figure 2.9: ICF as a function of the BPSK part of the mixed signal.

It can also be noted that the ICF for a mixed signal are below 0 even when only a relatively small part of the signal is BPSK modulated.

2.7 Conclusions

The possibility of using the ICF for different kinds of interfering signals is studied. The ICF correction factor is derived for a pulsed signal and it is interesting to evaluate the validity for different kinds of pulsed signals as well as other kinds of interfering signals. The ICF correction factor is useful for different kinds of pulsed signals, such as periodic pulses with real amplitude or random phase as well as pulsed signals with random phase and arrival time.

For signals consisting of several pulsed signals the ICF correction factor is too low when the number of signals is large. However if the ICF is positive the result from using the correction is always better compared to not using it. When a pulsed signal is mixed with a BPSK modulated signal, the ICF is too affected by the BPSK part of the signal and hence yield a correction factor that is lower than desired.

3 Interference Temperature and Network Analyses

3.1 Introduction

Traditionally the consequences from intersystem interference are often analyzed at link level, in terms of signal to noise ratio or bit-error probability in the receiver, see chapter 2. However, with the development of new flexible radio systems it has been increasingly important to be able to analyze the effects of intersystem interference on higher system levels. Since the performance on an individual link might no longer be the determining factor for the quality that the operator experiences it is important to be able to estimate the impact of the intersystem interference on a network, and the services the network supports [16].

To illustrate the effects of intersystem interference on an ad hoc network we study how the distribution of Situation Awareness (SA) information is effected by the intersystem interference in a tactical scenario. To get better statistical base for our conclusions we also investigate how the network connectivity and throughput is affected by different levels of intersystem interference for a large set of random networks.

3.2 Intersystem Interference model

The interference source used is a computer satisfying the standard EN55022 class B [45], which is the maximum allowed radiated interference limit for information technology equipment sold within the European Union. For frequencies above 230 MHz the limit is 37 dBμV/m in 120 kHz bandwidth at 10 meters distance [2]. The disturbance power, P_{COTS} in the radio receiver can be estimated as [45]:

$$P_{\mathrm{COTS}} = \frac{\lambda^2}{4\pi Z_0} pqG_{\mathrm{R}} E_{\mathrm{R}}^2(r), \qquad (3.1)$$

where λ is the wavelength [m], Z_0 is the wave impedance for free space (= 377 Ω), p is the polarization matching factor $0<p\leq 1$, q is the matching factor between radio antenna impedance and load impedance $0<q\leq 1$, G is the antenna gain of the receiving antenna in the direction of the disturbance, $E(r)$ is the electrical field strength [V/m] of the disturbance at the receiver antenna and r is the 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. If we assume that the interference has a constant power spectral density, the spectral density can be expressed as

$$N_{\mathrm{I}} = \frac{P_{\mathrm{COTS}}}{W}. \qquad (3.2)$$

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 is given at a distance of 10 meters. If we want the field strength at another distance, for example 3 meters, the field strength can be calculated as

$$E_{\mathrm{R}}(3) = \frac{10 \cdot E_{\mathrm{R}}(10)}{3} = \frac{10 \cdot 10^{37/20} \cdot 10^{-6}}{3} \tag{3.3}$$

where the limit for the field strength in the standard is 37 dBμV/m. The wavelength of the disturbance is the speed of light divided by the frequency of the disturbance. We are interested of the frequency 300 MHz, which yields a wavelength of one meter. We also assume that *p* and *q* equals one. With a bandwidth of 120 kHz and an antenna gain assumed to be one, the power spectral density is obtained as

$$\begin{aligned} N_{\mathrm{I}} &= \frac{P_{\mathrm{COTS}}}{W} = \frac{\lambda^2}{4\pi Z_0} pqG_{\mathrm{R}} \frac{E_{\mathrm{R}}^2(3)}{W} \\ &= \frac{(c/f)^2}{4\pi Z_0} pqG_{\mathrm{R}} \frac{\left(10/3 \cdot E_{\mathrm{R}}(10)\right)^2}{W} = 9.8 \cdot 10^{-17} \end{aligned} \tag{3.4}$$

We want to express the noise and interference in the receiver 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 N_0 is the spectral density of the noise in the receiver and kT_0= -204 dBW/Hz. The spectral density of the noise N_0 is equal to kT, where k is Boltzmanns constant and T is the noise temperature. A new noise figure can be calculated for the receiver when interference is present. This is done by adding the spectral density of the disturbance is added to the spectral density of the noise so that

$$F = \frac{N_0 + N_{\mathrm{I}}}{kT_0} \ . \tag{3.5}$$

With the interference present a new noise figure can be calculated. See Figure 3.1 for a plot of the power spectral density as a function the distance the intersystem interference.

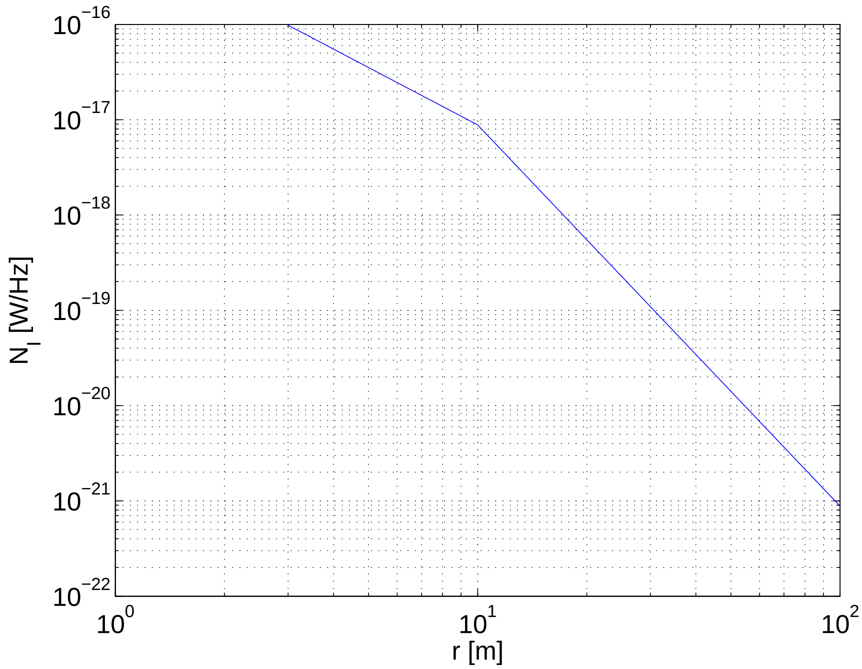


Figure 3.1: The power spectral density as a function the distance the intersystem interference

3.3 Radio Network Model

3.3.1 Link model

An essential part of modeling an on-ground or near-ground radio network is the electromagnetic propagation characteristics due to the terrain variation. A common 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 a uniform geometrical theory of diffraction (UTD) model by Holm [37]. To model the terrain profile, we use a digital terrain database with a resolution of 25×25 m for terrain type and 50×50 m for height data. All our calculations of the basic path-loss are carried out using the wave propagation library DetVag-90® [38].

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 interference and noise ratio (SINR), Γ_{ij}, here defined as $E_b/(N_0+N_I)$ in node v_j as

$$\Gamma_{ij} = \frac{PG_iG_j}{(N_0 + N_I)L_b(i, j)R}, \quad (3.6)$$

where P denotes the power of the transmitting node v_i (equal for all nodes), G_i is the antenna gain in the transmitter , G_j the antenna gain in the receiver, N_0 and N_I is the spectral density of the noise and interference respectively, 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 SINR is not less than a threshold γ_0, i.e. $\Gamma_{ij} \geq \gamma_0$.

3.3.2 Medium Access Control

In this study we will use a Time Division Multiple Access (TDMA) based Multiple Access Control protocol see [40]. TDMA is a static, collision-free, protocol where the channel sharing is done in the time domain. We choose here 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. However, how the scheduling is done in a mobile scenario is by itself a research area. The aim here is not to investigate how such scheduling of the Medium Access Control (MAC) protocol should be done. However, we want a schedule that adapts to the traffic and the network topology in order to study the effects of intersystem interference. Therefore, we use a rather optimal method to decide which node may use a certain slot and do not consider the required control traffic. According to this method, we determine at the beginning of each time slot, which node has the oldest queued packet. This node is then allowed to use the time slot. The protocol is also traffic adaptive, i.e. the node is allocated time slots corresponding to the traffic load the node is exposed to. For simplicity, the slot assignment in our simulation is centralized [39], there are however ways to distribute the slot assignment, see [40].

3.3.3 Routing Protocol

To find suitable routes in the tactical scenario we use the Fisheye State Routing (FSR) protocol. The FSR protocol is a proactive link state protocol whose objective is to keep control traffic low and still provide accurate information about the routes, see [41]. The FSR protocol uses the Fisheye technique, which was originally used to reduce data required to represent graphical data. A node's perception of its surroundings, according to this technique, 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.

To find suitable routes in the random networks we use an optimal minimum cost routing, which is here solved with Dijkstras algorithm. Furthermore we ignore the cost of finding the routes.

3.3.4 Distributing SA Information

In the tactical scenario we choose the implement the SA service with help of the FSR protocol. When using a proactive routing protocol, such as 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 [43]. An efficient method of distributing SA data might thus be to ”piggyback” the SA data onto existing control traffic. Since our current implementation of the 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.

3.3.5 Unicast Traffic Model

In our study of the effects of intersystem interference in the random networks we choose to assume unicast traffic, i.e. a packet has a single source and destination. We assume that packets of equal size arrive to the network according to a Poisson process, with arrival rate λ. That is, on average λ packets per slot arrive to the network. Furthermore we assume that the traffic is uniformly distributed over the nodes, i.e. each node is equally probable as source node and each node except the source node is equally probable as destination node.

3.4 Performance Measures

3.4.1 Tactical scenario

In the tactical scenario we choose to use the average service availability [39], for the SA-service as a performance measure. Furthermore we choose to divide the vehicles in two groups, one with vehicles less than 3 km away, and one with vehicles more than 3 km away. We also present the service availability for the command vehicles.

3.4.2 Random Networks

To evaluate the effect on performance from intersystem interference we use the connectivity, ρ [39], and the maximum network throughput, λ^* [packets/slot], as performance measures. We define the network connectivity as the probability that two randomly chosen nodes can communicate, i.e. there exist a route between them. Furthermore, we define λ^* as the largest input traffic arrival rate for which the network delay is finite, and for this measure we can derive an analytic approximation, [44] .

The maximum number of packets/slot that can be transmitted by node i is μ_i, which we approximate by the fraction of the time slots that are assigned to node i, i.e.

$$\mu_i = \frac{\Lambda_i}{\sum \Lambda_i}, \tag{3.7}$$

where Λ_i is the number of routes that traverses node i.

To calculate the traffic load, λ_i, on node i we note that when the network connectivity is ρ there are a total of $\rho N(N\text{-}1)$ point-to-point connections in the network, where N is the number of nodes. Since there are Λ_i routes that traverses node i and we have uniform traffic we can write λ_i as

$$\lambda_i = \frac{\lambda}{\rho N(N-1)} \Lambda_i . \tag{3.8}$$

The network is stable if $\lambda_i \le \mu_i \ \forall\ i$. The maximum throughput is reached when the condition is met with equality for at least one node. The maximum throughput in packets per time slot can therefore be written as

$$\lambda^* = \min_i \left(\mu_i \frac{\rho N(N-1)}{\Lambda_i} \right) = \frac{\rho N(N-1)}{\sum_i \Lambda_i} . \tag{3.9}$$

The maximum throughput can be interpreted as one over the average route length. We estimate the network connectivity and the maximum network throughput, for a number of independent networks, and denote the estimated average values with $E[\rho]$ and $E[\lambda^*]$.

3.5 Simulation Set-up

3.5.1 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 companies each with 24 vehicles, one command and artillery company with 20 vehicles, and one pioneer and support company with 39 vehicles. Altogether, we then have 155 vehicles, or communication nodes. The scenario is drawn up for armed combat on Swedish ground. The tactical scenario and details about how the units are moving are described in [37].

In the scenario the task for the mechanised battalion is to strike out a hostile air-landing within an area assigned to the battalion, and be prepared to strike out such an air-landing in adjacent areas. The area around Skara is selected, where most parts of the terrain are rather flat and covered by meadows and groves. First the unit 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.

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 values of the parameters that are fix under our simulations of the tactical scenario is set according to Table 1.

Table 3.1: Parameters used in the simulations.

P	$G_T(i,j)$	$G_R(i,j)$	kT_0	γ_0
50 W	1	1	4×10^{-21} W/Hz	15 dB

3.5.2 Random Networks

We have simulated 512 different stationary networks consisting of 16 nodes, uniformly distributed over an area of 1·1 km see Figure. 3.2. In the network a number of nodes (0, 4, 8, and 16) are subjected to intersystem

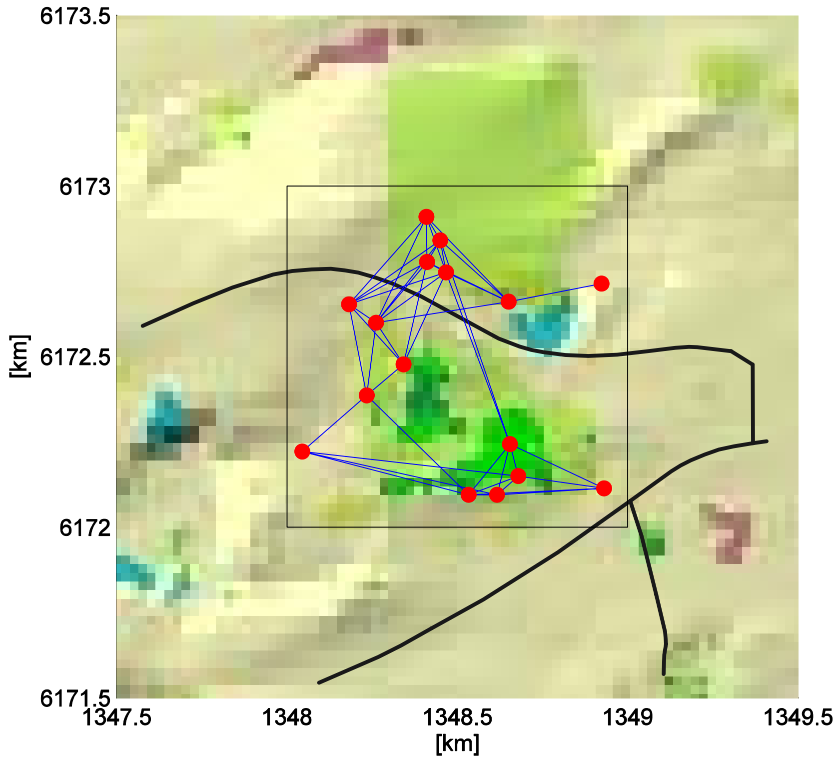


Figure. 3. 2: One of the 512 different networks.

interference. For each of the 512 networks and each number of interfered nodes the nodes with interference are randomly chosen 16 times. For each network we have also chosen the transmitter power P so that the connectivity of the network fulfills our requirements. The values of the parameters that are fix under our simulations of the tactical scenario is set according to Table 2.

Table 3.2: Parameters used in the simulations.

$G_T(i,j)$	$G_R(i,j)$	kT_0	γ_0
1	1	4×10^{-21} W/Hz	15 dB

3.6 Simulation Results

3.6.1 Introduction

In this section we present the results of our simulations. We first present the results for the SA-service in the tactical scenario. We then present our results concerning the network connectivity and throughput for the random networks.

3.6.2 Tactical Scenario

In figure 3.1 we present the results for the situation where all vehicles have intersystem interference and in Figure 3.2 we present the results for the situation where only the command vehicles have intersystem interferences.

In both figures we represent the represent the service availability for vehicles closer than 3 km away with solid red lines and vehicles more than 3 km away with solid blue lines. Furthermore we represent the service availability for the command vehicles closer than 3 km away with dashed red lines and command vehicles more than 3 km away with dashed blue lines.

If we first consider Figure 3.1 we can se that the service availability, as expected, decreases with increasing intersystem interferences. The service availability for the vehicles closer than 3 km is only slightly affected for moderate levels of intersystem interferences. However, the service availability for the vehicles more than 3 km away is reduced even at moderate levels. This difference in manly due to that the service availability for vehicles more than 3 km away is more dependent on long links which are more vulnerable for intersystem interference.

If we compare the service availability for all vechiles in the network with the service availability for the command vehicles (dashed/solid lines) we can see that there is almost no difference for the vehicles more than 3 km away. However, for vehicles less than 3 km away the service availability is lower for the command vehicles than for the average vehicle. This is probably due to the fact that the command vehicles are moving more autonomously than the other vehicles in the scenario, i.e. they have longer links to their neighbors.

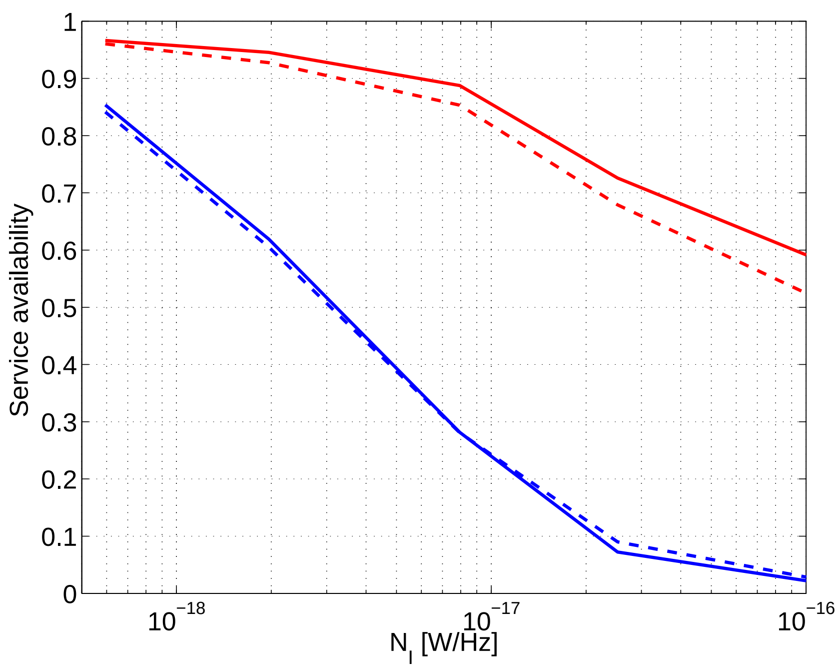


Figure 3.3: Average service availability for vehicles in the scenario where all vehicles have the same intersystem interference. The {**red, blue**} lines represent the average service availability for {**R < 3 km**, **R > 3km**} in the battalion. The dashed version of the lines represents the service availability for the command vehicles.

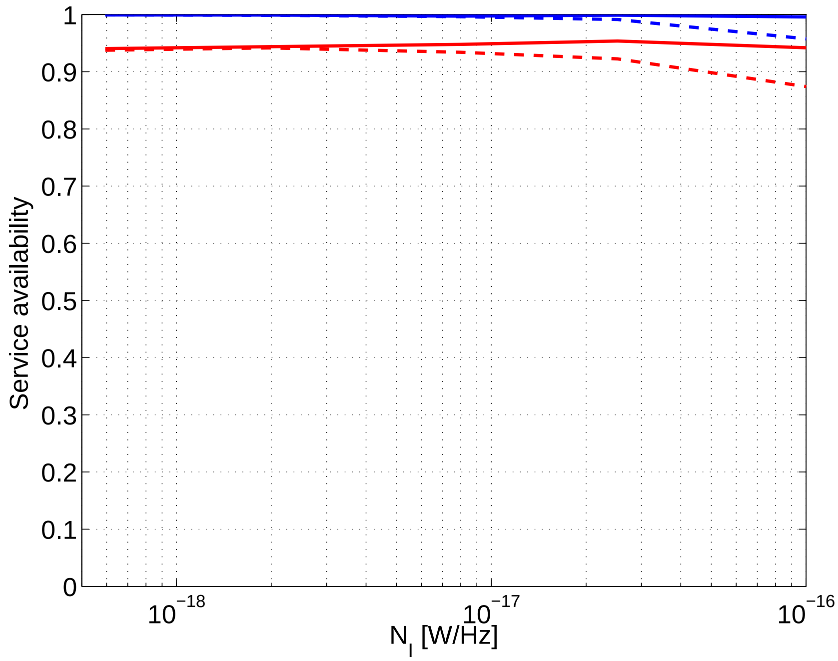


Figure 3.4: Average service availability for vehicles in the scenario when only the command vehicles have intersystem interference. The {**red, blue**} lines represent the average service availability for **{R < 3 km**, **R > 3km**} in the battalion. The dashed version of the lines represents the service availability for the command vehicles.

However, the service availability for the scenario where only the commanding vehicles have intersystem interfere is hardly affected at all when we increase the intersystem interference, even when we consider the service availability for the commanding vehicles, see Figure 3.4. From this we can conclude that even if a vehicle loses links, due to intersystem interference, the vehicles service availability can be unaffected as long as the vehicle 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 also considered the network capacity the SA service would probably be affected in a negative way by the intersystem interference.

From Figures 3.3 it can also be seen that when there is intersystem interference at all nodes, the average service availability varies more rapidly with the interference level. In the latter case it requires approximately 5 dB change in the interference level to cause a 25% units change of the average service availability. To obtain a level of 10 percent units the uncertainty in SIR must be below approximately 2-3 dB. In figure 2.1, it is shown that the difference in SIR between an AWGN and a pulsed signal can be 20 dB for a constant BEP. The conclusion is that if the Gaussian approximation is used for pulsed interference without any correction for the waveform properties, the error in the estimated average service availability can be in the order of 90% in that case. With use of the ICF, the error in interference level can be reduced to a few dB which gives an error in average service availability in the order of 10-20% if there is intersystem interference at all nodes.

3.6.3 Random Networks

To get better statistical base for our conclusions we will now study how the network connectivity and throughput is affected by different levels of intersystem interference for a large set of random networks. Two cases are investigated, one where the network always is connected and one where the network falls apart.

For the case when the network is connected the network connectivity is always one for all levels of interference and number of interfered nodes (hence, not shown in a figure). In Fig. 2 the estimated average of the maximum throughput, $E[\lambda^*]$, is shown as a function of the spectral density of the interference, N_I. The blue line is the reference system with no intersystem interference and the cyan line is when all nodes in the network have intersystem interference.

When the interference level increases there are fewer links and hence longer routes, which leads to lower throughput. When the number of nodes with interference goes from 0 to 4 the effect on throughput is larger than for the case from 4 to 8. This depends on the different route lengths before and after more nodes with interference are added. With no intersystem interference the network is highly connected with short routes and hence there are not many alternative routes with the same length, e.g. there is only one route between two nodes with length one. In the case when we have 4 nodes with interference the routes are longer and there are probably several routes with the same length. Hence, the first nodes with interference that are added cause the largest decrease in throughput.

In the second case we have a network that is barley connected, i.e. even a low interference will result in that the network falls apart, see Figure. 3.5, where the estimated network connectivity $E[\rho]$ is shown. In Figure 3.6 we can observe that the connectivity for networks where all nodes have interferences decreases to zero when the intersystem interference level increases, i.e. the networks fall apart completely. However, when only 4 or 8 nodes have intersystem interference the estimated network connectivity decreases slower because the network forms small subnets that internally are connected by the nodes without intersystem interferences. We can also observe that the first nodes with interference cause the largest decrease in connectivity in absolute terms. This is probably due to that if the network falls apart in two equal parts the network connectivity is ½, while if the network falls apart in 4 equal parts the network connectivity is ¼. The difference in connectivity thus gets smaller, in absolute terms, when more intersystem interference is introduced in the network. In this case, with a network with low connectivity, the throughput increases with increased intersystem interference, since the network forms subnets with shorter routes when the

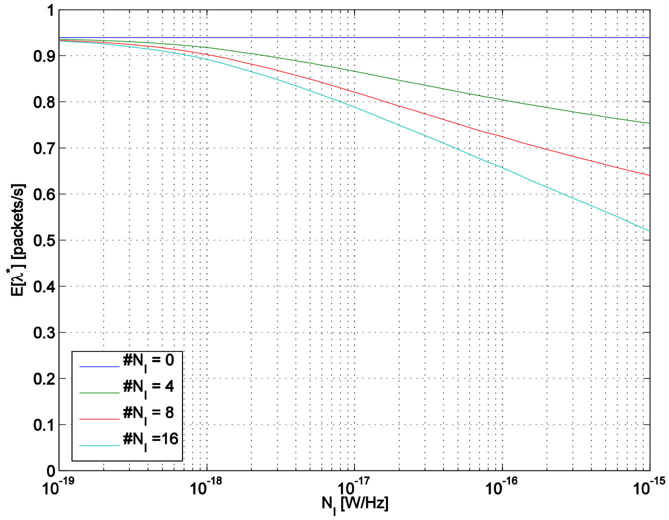


Figure 3.5: Estimated average maximum throughput as a function of the spectral density of the interference for networks with high connectivity.

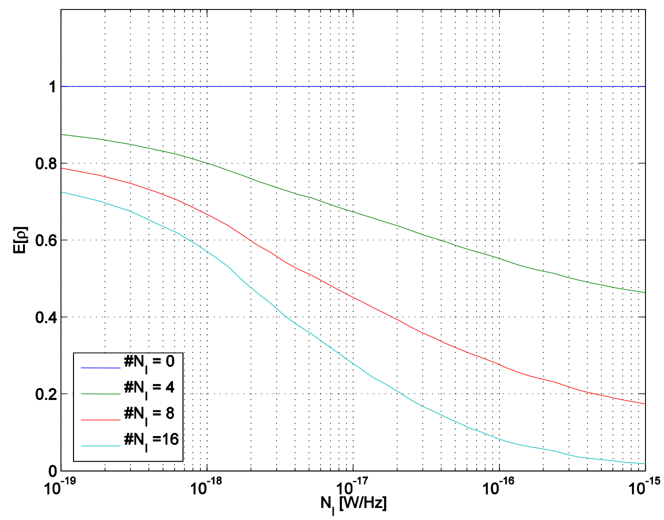


Figure 3.6: Network connectivity as a function of the spectral density of the interference for networks with low connectivity.

network falls apart. As the intersystem interference level increases the subnets gets smaller with shorter routes and hence higher throughput. However, it is important to recognize that all nodes do not share the increase in throughput since the connectivity is lower than one.

3.6.4 Conclusions

In this chapter we have investigated how the SA-service in a tactical scenario is affected of intersystem interferences. We have also studied how the connectivity and throughput is affected by intersystem interferences for a set of random networks.

From the simulations of the tactical scenario we conclude that intersystem interference in all units in a battalion can strongly reduce the availability of a SA service. It is also shown that intersystem interference that is present only in the commanding vehicles will only result in minor changes in the service availability. However, reduction in service availability does not only affect the commanding vehicles, despite that they cause the intersystem interference.

Our study of intersystem interference in random networks show that the effect on the condition of the network without intersystem interference. For a network that is fully connected even with intersystem interference the throughput in the network is decreased. In other more instable networks the intersystem interference yields a decrease of the network connectivity, and the network falls apart into subnets. For both cases the largest changes often occur when the first nodes are affected by intersystem interference.

Since intersystem interference can affect an ad hoc network in different ways it is important to perform network simulations were the intersystem interference is incorporated.

4 Effects of Intersystem Interference on Trust in SA Services for Mechanized Battalions

4.1 Introduction

An important aspect of situation awareness in many real-time environments is the perception of the environment, such as the position of objects and obstacles relative own position, comprehension of the meaning of this information, and projection of events or actions in the future based on this perception and comprehension (Endley, 1995)[25]. While operators in some domains have benefited from advanced sensor and information presentation technologies to enhance the situation awareness of the environment, such technologies have usually not been available for front-end personnel in the emergencies and public safety domain. For example, Fogel et al. (2004)[26] and Lindgren et al. (2004)[30] describe how breathing apparatus (BA) rescue personnel currently use verbal communication to create shared reference points for further orientation and to recover from disorientation. When visibility is severely restricted they even prefer to follow internal walls using tactile feedback and take each others hand to avoid disorientation.

There is, however, an increased interest in information presentation technologies and positioning services that allow the rescue personnel to navigate more freely. For example, Figure 4.1 shows a helmet-mounted display (HMD) for rescue personnel that is developed by a research group at UC Berkely (Wilson et al., 2005)[36]. The HMD can be used for presenting information such as floor plan, hazards, and location of victims. For further support of the situation awareness, a positioning service may also be included based on GPS information that shows own and other personnel's position within the floor plan. The current generation of GPS equipment do not function indoors, but recent developments of signal processing techniques may enable an indoor capability (van Diggelen & Abraham, 2001; Dedes & Dempster, 2005)[35][24]. Once indoor GPS equipment is commercially available, it can be used to develop advanced positioning services for presentation on a HMD.

The problem when introducing a positioning service for own and other personnel's position is that the digital radio communication for distributing the GPS information may be compromised due to intersystem interference. Electronic emissions from other components, such as power sources and information technology equipment, may simply add noise in the frequency spectrum for radio communication and thereby reduce the communication capability. GPS indoor equipment is particularly sensitive to intersystem interference since 20 dB of the signal strength is lost (Brickerstaff et al., 2005)[23]. With severe intersystem interference, the quality of the positioning service may decrease to a point that hampers the situation awareness and eventually the user's trust in the presented information. Since intersystem interference can have so dramatic consequences, FOI have recently studied the effects of intersystem interference on trust in a positioning service for a mechanized battalion. Linder et al. (2004)[16] show that even for modest levels of intersystem interference, there are situations with significant position errors that hamper the commander's ability to control the battalion. Further, the results indicate that intersystem


Figure 4.1: a) Position of HMD, b) Concept illustration of floor plan presentation

interference may increase the risk for fratricide, although the risk should be interpreted cautiously due to a limited analysis. Although not specifically intended for rescue personnel, the purpose of this paper is to illustrate the effect of intersystem interference on positioning services by refining the results from Linder et al. (2004)[16]. An additional analysis was also performed of the special cases when the battalion commander directly supports a company commander about where to position individual vehicles. The methodology used may serve as an example for how to investigate the risks for intersystem interference in a positioning service for rescue personnel. First, the general characteristics of trust are described as a basis for assessing the effects of intersystem interference. Thereafter follows the mission objectives and organization of mechanized battalions. Finally, the current evaluation of trust in the positioning service is described.

4.2 Characteristics of Trust

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 (see Luhman, 1980; Lee & See, 2004)[31][29]. Continuously doubting the available information simply requires too much mental effort and hinders timely actions. Trust is a multi-dimensional concept that integrates information from three levels of abstraction regarding the system's support of the operator's goals: performance, process, and purpose (Lee & See, 2004)[29]. The performance level refers to the system's behavior to support the operator's goals. The process level, on the other hand, refers to whether the system's principles of operation are acceptable. Finally, the purpose level refers to the system's underlying motives and intentions. The abstraction levels are also related so that behavior provides information about underlying processes which in turn provide information about the underlying motives and intentions. Similarly, knowledge about motives and intentions create expectations on behavior. Finally, the user's perceptions of all abstraction levels are integrated into a continuous perception of trust (Muir, 1994)[32]. How robust the perception is depends on the type and number of abstraction levels that are integrated. More abstraction levels improve the robustness. Especially, when there is knowledge about underlying motives and intentions (Rempel m.fl., 1985)[33].

Failure to instill trust is particularly important for a positioning service since operators otherwise will likely resort to using voice communication which is viewed as the main backup communication system in a mechanized battalion (see Fransson et al., 2002)[28]. The problem is that voice communication consumes considerably more bandwidth than the digital positioning service. On the other hand, operators may also place too much trust in the positioning service if they do not consider uncertainties that may affect performance. Trust should thus be well calibrated to the actual capabilities for the most efficient utilization of the positioning service. Unfortunately, environment, interference, etc. that may affect the quality of the positioning service are often not directly observable which may reduce the predictability of the communication system.

Since trust is important for many military applications, a research program was recently established at FOI (Andersson et al., 2003)[22]. Table 4.1 shows some dimensions of trust that were identified in the initial literature survey. Studies at FOI show that military operators' trust is mostly based on the system's capability which is consistent with available theories (Thuren et al., 2005)[34].

Table 4.1: Dimensions of trust

Level of abstraction	Trust dimension
Performance	*Capability*: Capacity to function in situations that are important for the mission
	Predictability: Knowing how the system is going to react based on observations and experience
	Reliability: Functionality in difficult and dangerous situations
	Robustness: Ability to function when damaged or distorted
	Usefulness: The system's practicality and applicability
Process	*Dependability*: The system's capability to fulfil its task in situations where it may be unreliable
	Understanding: Knowing how the system "thinks" and operates
Purpose	*Intentionality*: The system's purposes are congruent with the expectations, that is there are no hidden agendas
	Responsibility: The system is accountable and is not trying to blame others or find scapegoats

4.3 Mechanized Battalion

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 Combat Vehicle 90, an armored personnel carrier (APC), or three Combat Vehicle 122, a main battle tank. Each Combat Vehicle 90 carries an infantry group of six soldiers. The main mission objectives for a mechanized battalion are to take terrain or strike the opponent, although defense and delaying the opponent's advance are also important 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 where the distance between each vehicle is about 3 km to maximize the area coverage. Strike against airborne troops usually have less demands on coordination, since it is most important to attack the landing zone as soon as possible before the opponent can regroup and form coordinated combat units.

The battalion is commanded by the staffs L1, L2, and L3. L1 and L2 use Combat Vehicle 90's for the tactical command and control that accompanies the strike movement where as L3 is responsible for the strategic planning from containers. Each command and control vehicle has six seats for the battalion commander, intelligence officer, artillery commander, combat commander, and two assistants. The battalion's command and control is generally directed towards the area coverage of the companies rather than individual vehicles. The company commander provides command and control for the company in a time scale of 10-30 s while simultaneously participating in the battle. Finally, the time-scale for platoon command and control and direct combat is a few seconds. See Linder et al. (2004) [16]for more information about mechanized battalions.

Table 4.2: Size of target areas for mission objectives

Type of unit	Strike		Defense	Delay of advance
	Airborne (km^2)	With x Depth	With x Depth	Width x Depth
Mechanized battalion	500	3-6 x 3 km	5-10 x 3 km	10 x 30 km
APC company	120	1.0-1.5 km	2-3 x 1 km	2-5 x 10 km
APC platoon	30	300 m	500 m	NA
APC	10	100 m	100 m	NA
Tank company	120	1.5 km	5 x 1 km	5 x 15 km
Tank platoon	30	300 m	1 km	NA
Tank	10	100 m	100 m	NA

4.4 Simulation of Positioning Service for a Mechanized Battalion

An area near Skara was selected for a simulation of a strike against airborne troops. In the beginning of the scenario, the battalion is spread out to cover the anticipated drop zone. Once informed about the specific location of the drop zone, all combat vehicles move at high speed towards the drop zone 10-20 km away using available roads. The positioning service in this scenario was simulated using a multi-hop ad hoc network (Linder et al., 2004)[16]. The advantage of an ad hoc network is that no infrastructure has to be pre-deployed. Instead all nodes coordinate the exchange of GPS coordinates based on when the coordinates where measured. Thus, updated positions may be routed between vehicles without direct radio contact. The user requirements for errors in estimated position were 20 m for all vehicles within 3 km, 200 m for all vehicles within 3 to 15 km, and 500 m for vehicles beyond 15 km. However, since most vehicles where within 15 km, the 200 m requirement was used for vehicles beyond 3 km. The reason for the high demands on position error for vehicles within 3 km was to avoid fratricide without using a special identification system. The specific details of the ad hoc network simulation can be found in Linder et al. (2004)[16].

Four levels of intersystem interference were simulated, 10, 22, 33, and 44 dB, where 10 dB corresponds to no intersystem interference. The higher levels of intersystem interference correspond to having a computer fulfilling the emission level in EN55022 class B at distances of 20 m, 10 m, and 3 m. EN55022 class B is the maximum allowed limit of mediated emission from information technology equipment sold in the European Union. Further, data rates of 0.5, 1.0, and 2.0 Mbit/s were also simulated. Figure 4.2 and 4.3 shows the effect of 33 dB intersystem interference which corresponds to a computer at 10 m and a data rate of 0.5 Mbit/s. Only the same level of intersystem interference for all vehicles with 0.5 Mbit/s data rate is evaluated in this paper. See Linder et al. (2004) for information about intersystem interference only of command vehicles and other data rates. The figures show that the network connectivity decreases dramatically with a medium level of interference even at the lowest data rate. The network connectivity is still acceptable, however, within the platoons.

4.5 Evaluation of Positioning Service for a Mechanized Battalion

Since about 70 % of the voice communication in a mechanized battalion consists of position information (Alvå & Palmqvist, 2003), it is not surprising that operators are vary satisfied with the graphic presentation of vehicle positions (Fransson et al., 2002)[28].The purposes of the positioning service is to avoid fratricide and to facilitate coordination during battle. Avoiding fratricide requires very small position errors of less than 20 m for all vehicles that are within the range of direct fire, which is 3 km. There demands on the position error are less for coordination of vehicles at the higher levels of command, since they operate at longer timescales. For example, the battalion command and control is more concerned with the companies' area coverage and a position error of a few hundred meters does not matter (Fransson, 2004)[27]. However, in difficult situations the battalion commander may want support a company commander about where to position individual vehicles. An intermediate level of maximum position error is required in this situation to avoid confusion in communication between the battalion and company commander. Thus, a positioning service for a mechanized battalion serves at least the following functions:

- Battalion commander's coordination of the companies' area coverage.
- Battalion commander's support of company commanders about where to position individual vehicles.
- Avoiding fratricide for vehicles within line of sight and range of direct fire.

4.6 Avoiding fratricide for vehicles within line of sight and range of direct fire.

The purpose of this paper to evaluate how the positioning system supports the battalion commander's situation awareness and trust in the companies' area coverage as well as the direct support of company commanders. More information about avoiding fratricide using a positioning service can be found in Linder et al. (2004)[16]. 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, positioning service that is being developed for mechanized battalions in Sweden (Albinsson & Fransson, 2002)[20]. The hulls were interpolated in small steps to allow more detailed measurements. The position error in area coverage 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 4.4 illustrates the principle for measuring the position error of area coverage.

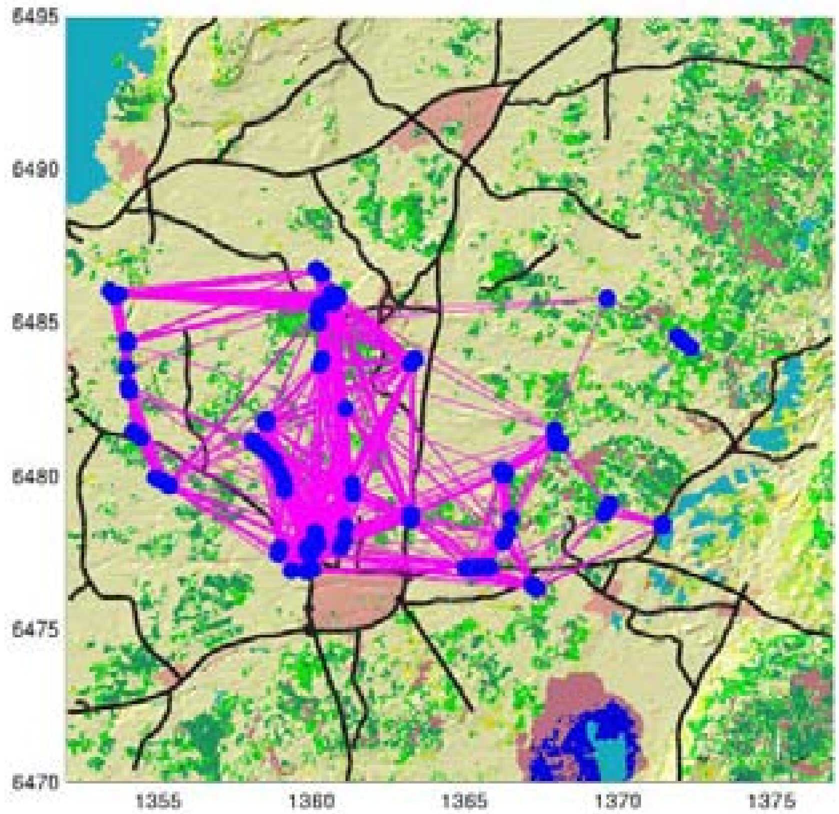


Figure 4.2: Connectivity of the network with no intersystem interference and a data rate of 0.5 Mbit/s.

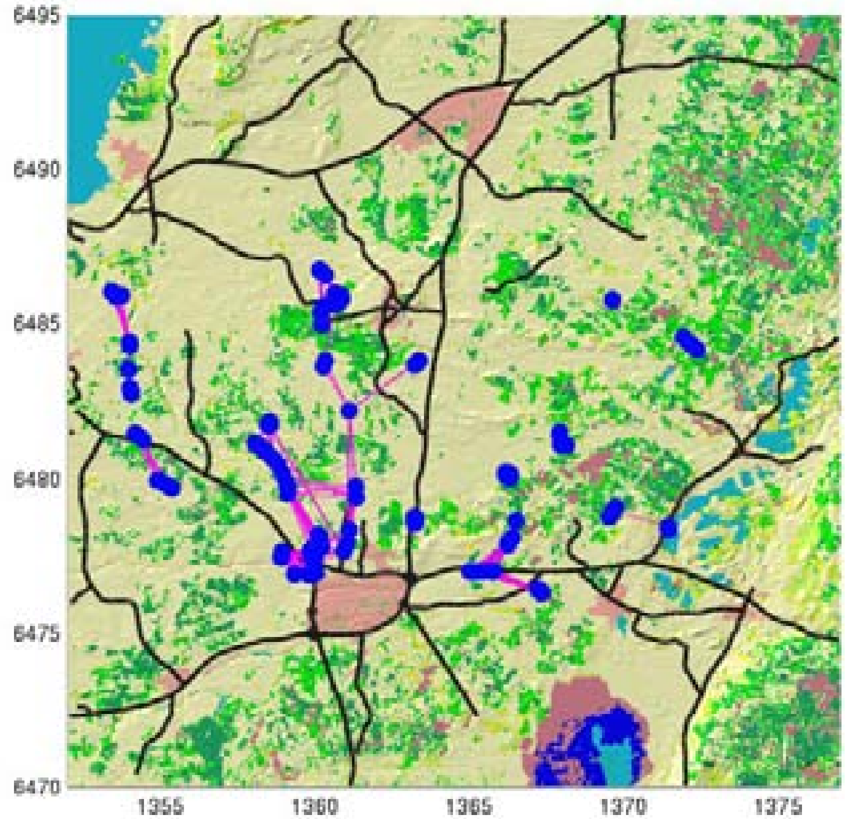


Figure 4.3: Connectivity of the network with 33 dB intersystem interference which corresponds to a computer at 10 m and a data rate of 0.5 Mbit/s.

Figure 4.5 shows how the position error of the companies' area coverage varied over the scenario for L1 with 33 dB intersystem interference of all vehicles and a data rate of 0.5 Mbit/s. The figure shows that the battalion commander has updated position information about company A and D for most of the scenario, intermittently loses contact with company B, and rarely has updated information about company C. A more overall view is provided in Table 4.3-4.5 that show how the intersystem interference affect the distribution of position error in area coverage for the battalion commanders at a data rate of 0.5 Mbit/s. The tables show a similar distribution of position errors in area coverage for all battalion commanders where even 22 dB of can cause position errors that are larger than 200 m. Only about 2 % of these errors are, however, larger than 500 meters which seriously can affect the battalion commanders' situation awareness. Although the percentage of position errors if fairly small, they occur intermittently which reduces the predictability of the positioning service. Further, it becomes increasingly difficult for the battalion commanders to maintain situation awareness with higher levels of intersystem interference. Almost a third of the position errors are larger than 200 m at 33 dB, and about 80% of the position errors are larger than 200 m at 44 dB. The majority of these errors are also larger than 500 m. It is therefore doubtful whether the battalion commanders will be able to exercise the proper control of the companies at 33 and 44 dB of interference. Finally, since L3 is stationery, it is surprising that the position error is

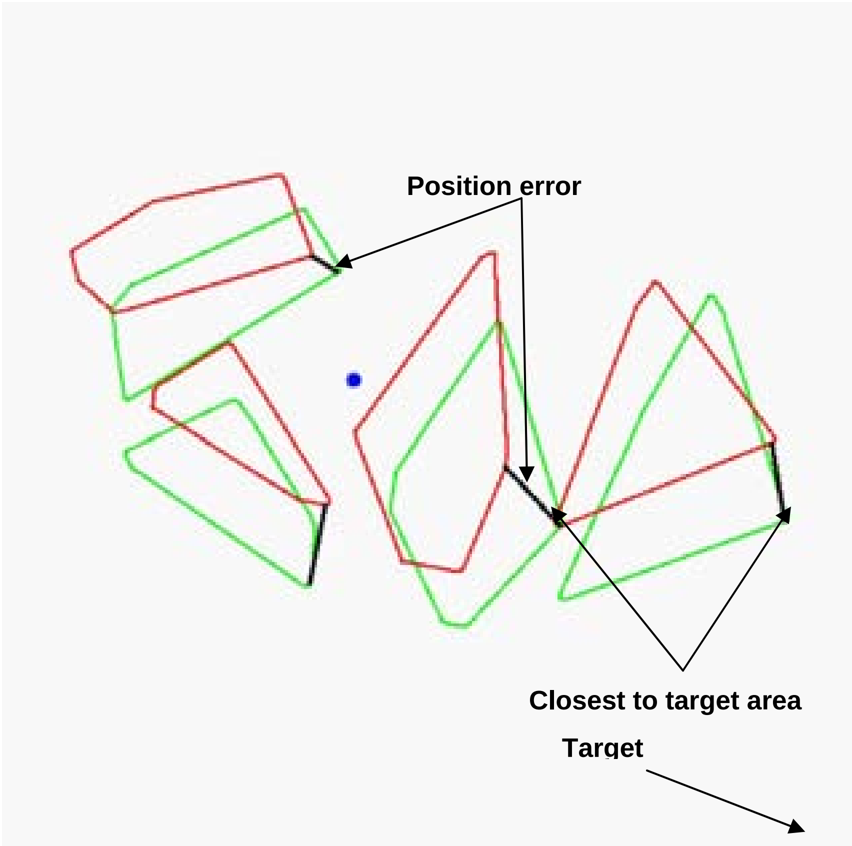


Figure 4.4: Principle for measuring position error of area coverage. The blue dot shows the position of the command and control vehicle. The green convex hulls represent correct position of the companies' area coverage. The red convex hulls represent the estimated position of the companies' area coverage.

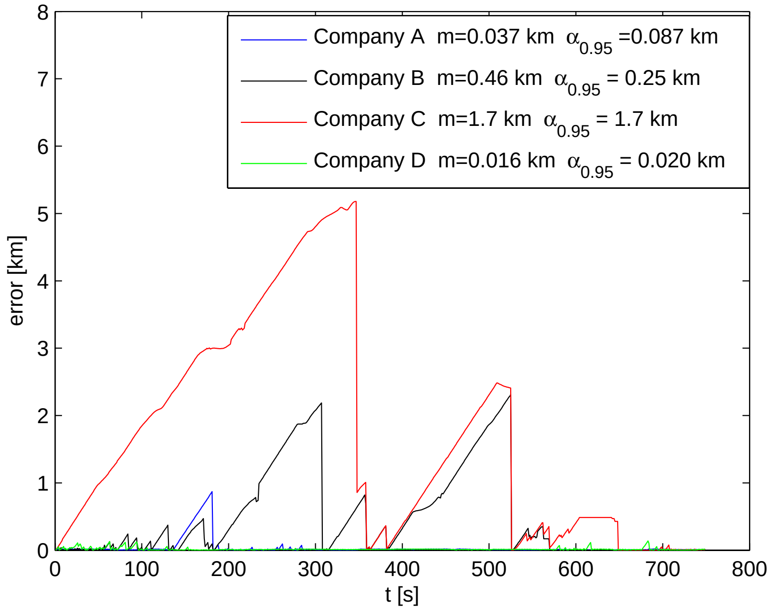


Figure 4.5: Position error of the companies area coverage for L1 at 33 dB intersystem interference of all vehicles and a data rate of 0.5 Mbit/s. The mean position error over the scenario is shown in the legend. The mean position error was calculated by excluding the 95 % percentile.

Table 4.3: Distribution of position error in area coverage as the percent of time over the scenario for L1 at a data rate of 0.5 Mbit/s. The effects of four levels of intersystem interference of all vehicles are shown 10, 22, 33, and 44 dB.

Level of Interference	Error Interval [m]			
	0-20	20-200	200-500	>500
10 dB	99.8	0.2	-	-
22 dB	90.5	5.1	2.7	1.7
33 dB	57.1	11.1	8.3	23.5
44 dB	12.0	6.7	6.6	74.7

Table 4.4: Distribution of position error in area coverage as the percent of time over the scenario for L2 at a data rate of 0.5 Mbit/s. The effects of four levels of intersystem interference of all vehicles are shown 10, 22, 33, and 44 dB.

Level of Interference	Error Interval [m]			
	0-20	20-200	200-500	>500
10 dB	99.8	0.2	-	-
22 dB	90.3	5.1	2.6	2.0
33 dB	54.4	13.0	8.5	24.1
44 dB	11.3	5.4	5.3	78.0

Table 4.5: Distribution of position error in area coverage as the percent of time over the scenario for L3 at a data rate of 0.5 Mbit/s. The effects of four levels of intersystem interference of all vehicles are shown 10, 22, 33, and 44 dB.

Level of Interference	Error Interval [m]			
	0-20	20-200	200-500	>500
10 dB	99.8	0.2	-	-
22 dB	90.7	5.0	2.9	1.4
33 dB	55.1	12.1	9.0	23.8
44 dB	13.2	7.3	7.0	72.5

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. A dependent measure of the position deviation for battalion commander’s support of company commanders about the positioning of individual vehicles was developed by measuring the difference between the battalion and company commander’s information about the estimated position for vehicles within the company. For example, L1’s position information for company A was compared to their company commander’s position information for company A, etc. Only combat vehicles were included in the analysis since they are most likely the focus of direct support from the battalion commander. Figure 4.6 how the average position deviation for direct support of each company varied over the scenario for L1 with 33 dB intersystem interference of all vehicles and a data rate of 0.5 Mbit/s. The figure shows that the position deviation is particularly problematic for company C and B with large deviations during most of the scenario. A more overall view is provided in Table 4.6-4.8 that show how the intersystem interference affect the distribution of position deviation in direct support of company commanders by the battalion commanders at a data rate of 0.5 Mbit/s. The tables are almost identical for all battalion commanders at 10, 22, and 33 dB of intersystem interference. The tables show that the deviation in estimated position is over 200 m for about 6 % of the time at 22 dB of intersystem interference. At 33 dB of intersystem interference, the deviation is over 200 m for about 30 % of the time and over 500 m for about 23 % of the time. At 44 dB if intersystem interference, the distributions are more polarized which means the units either have contact or are out of contact for a long time. There are, however, also some differences at 44 dB of intersystem interference where L2 have smaller deviations than both L1 and L3 which result in about 10 % higher percentage of errors in the 0-20 m error interval. For L1 and L3, the deviation is over 500 m for about 41 % of the time, where as for L2 the deviation is only over 500 m for about 33 % of the time. Even only 22 dB of intersystem interference of all vehicles does thus result in differences in estimated position that may create confusion between the battalion and company commanders about the position of individual vehicles. Further, at least one out of three vehicles has a deviation over 500 m at 33 and 44 dB of intersystem interference. Such large deviations may clearly affect the possibilities to create a shared situation awareness and thus trust in the positioning service. Finally, the fewer deviations in the 0-20 m interval for L1 and L3 at 44 dB than at 33 dB of intersystem interference can be attributed to that the deviations are based on estimated positions and the non-optimal nature of the routing protocol.

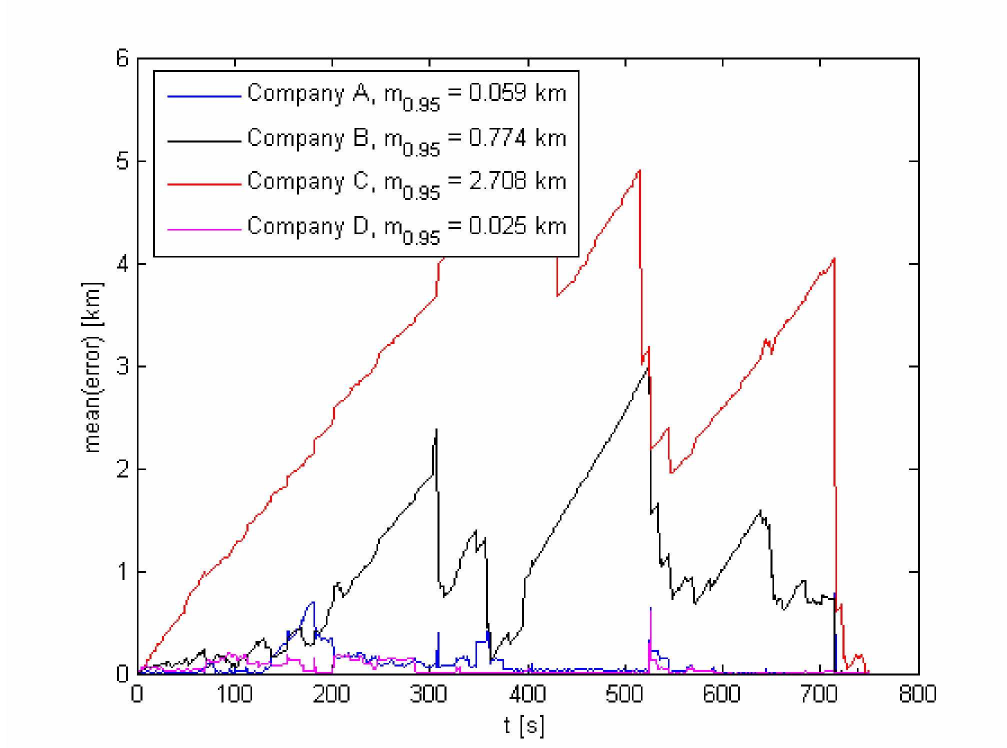


Figure 4.6: Average position deviation of L1's support of company commanders at 33 dB intersystem interference of all vehicles and a data rate of 0.5 Mbit/s. The mean position deviation over the scenario is shown in the legend. The mean position deviation was calculated by excluding the 95 % percentile.

Table 4.6: Distribution of position deviation in L1's support of company commanders as the percent of time over the scenario for L1 at a data rate of 0.5 Mbit/s. The effects of four levels of intersystem interference of all vehicles are shown 10, 22, 33, and 44 dB.

Level of Interference	Error Interval [m]			
	0-20	20-200	200-500	>500
10 dB	99.5	0.5	-	-
22 dB	82.8	11.4	4.4	1.4
33 dB	51.1	19.9	6.6	22.4
44 dB	49.2	6.7	3.5	40.6

Table 4.7: Distribution of position deviation in L2's support of company commanders as the percent of time over the scenario for L2 at a data rate of 0.5 Mbit/s. The effects of four levels of intersystem interference of all vehicles are shown 10, 22, 33, and 44 dB.

Level of Interference	Error Interval [m]			
	0-20	20-200	200-500	>500
10 dB	99.5	0.5	-	-
22 dB	83.2	11.1	4.4	1.3
33 dB	50.9	19.3	6.7	23.1
44 dB	58.0	5.7	2.8	33.5

Table 4.8: Distribution of position deviation in L3's support of company commanders as the percent of time over the scenario for L3 at a data rate of 0.5 Mbit/s. The effects of four levels of intersystem interference of all vehicles are shown 10, 22, 33, and 44 dB.

Level of Interference	Error Interval [m]			
	0-20	20-200	200-500	>500
10 dB	99.5	0.5	-	-
22 dB	82.7	11.4	4.8	1.1
33 dB	48.9	21.9	6.5	22.7
44 dB	46.1	9.3	3.7	40.9

4.5 Conclusions

The results confirm the reported effects in Linder et al. (2004) [16], that even for low data rates and levels of interference that affect all vehicles, there are situations where the battalion commander may not be able to control the companies. The effects are particularly disturbing for direct support of company commanders where a few companies may have large deviations for several minutes. While the requirements and also effects of intersystem interference are less for position information about the companies' area coverage, 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. When the interference increases further, both measures become unacceptable. The large percentage of position errors in area coverage that are greater than 500 m means that the position information is rarely updated, at least for a few companies. Similarly, the large percentage of position deviations that are larger than 200 m means that the position information is insufficient for direct support. Higher levels of intersystem interference therefore clearly hamper the battalion commanders' ability to control the companies. While the results indicate that higher levels of intersystem interference may reduce the battalion commanders' situation awareness and trust in the positioning service, these results need to be validated by asking subject matter experts for subjective ratings of how they experience the positioning services on an appropriate scale of trust. Further studies should also include a line of sight measure to verify if there actually is a risk for fratricide as reported by Linder et al. (2004) [16]. Finally, further studies should consider a measure of the intermittent nature of position errors and deviations which may affect the battalion commanders' trust.

5 OPNET Modeler as platform for a future intersystem-interference analysis tool.

A feasibility study [18] has been performed in order to investigate if the network simulation tool OPNET Modeler is a possible alternative as a platform for a future intersystem-interference analysis tool. The conclusion is that OPNET Modeler is an alternative if simplified models of the intersystem interference within platforms can be used. Such simplified models must be based on a Gaussian approximation of the interference signal combined with an impulsiveness correction factor as discussed in chapter 2. If not the Gaussian approximation can be used as a simplified model, OPNET Modeler is not convenient as a basis for the intersystem-interference analysis tool. However, the impulsiveness correction factor makes it possible to use the Gaussian approximation without making large errors in the estimated bit error probability. A more detailed discussion is done in [18].

6 Publications within the project

The project has resulted in a number of publications. These publications are listed below.

Peter F. Stenumgaard, Leif Junholm, “Higher-Order Effects of Radiated Interference - Future Challenging Research Domains within EMC in Dynamic Wireless Communication Networks”, *EMC 2005 Zurich, International Symposium on Electromagnetic Compatibility*, Februari 2005.

Ulf Sterner, Sara Linder, “Effects of Intersystem Interference on a Situation Awareness Service in a Mobile Ad Hoc Network”, Proceedings of *RVK* -05, 14-16 June, Linköping, Sweden 2005.

Leif Junholm, Peter Stenumgaard, ” Higher-Order Effects of Radiated Interference - Future Challenging Research Domains within EMC in Dynamic Wireless Communication Networks”, *EMC Europe 2005, Workshop on Electromagnetic Compatibility in Wireless Communication Systems*, Rome, Italy 19-21 September 2005.

Peter F. Stenumgaard, Leif Junholm, “Higher-Order Effects of Radiated Interference - Future Challenging Research Domains within EMC in Future Military Dynamic Wireless Communication Networks”, *MILCOM 2005,* Atlantic City, USA, October 2005, U602-6.

Ulf Sterner, Sara Linder, “Intersystem Interference in mobile ad hoc networks”, *EMC Europe 2005, Workshop on Electromagnetic Compatibility in Wireless Communication Systems*, Rome, Italy 19-21 September 2005.

Peter F. Stenumgaard, “A Simple Impulsiveness Correction Factor for Control of Electromagnetic Interference in Dynamic Wireless Applications”, Accepted for publication in *IEEE Communication Letters.*

Peter Svenmarck, Karina Fors, “Effects of Intersystem Interference on Situation Awareness and Trust”, To be presented at *EPS, Emergency & Public Safety*
18 - 19 januari 2006, Gothenburg, Sweden

7 Conclusions

Future dynamic wireless applications require the ability to handle the problem of dynamic interference control or dynamic interference avoidance. A key issue is the ability to consider the total electromagnetic interference within the receiver band of a wireless communication system. Methods considering the total interference environment must be developed for instance in order to allocate frequency spectrum dynamically on demand. Such methods must be of low complexity to be useful in on-line applications so a simple but useful method is tractable to find. One such method is to use the total interference average power within the receiver bandwidth as a decision parameter to judge whether or not the interference level is low enough for using the channel. This method is based on the underlying assumption that the interference signal can be approximated as white Gaussian noise within the receiver band. To make this method useful, it is important to be able to make some adjustment for the actual interference waveform behind this interference power. Since different signal waveforms, given a fixed power, can give considerable differences in the bit error probability of the disturbed system, it is convenient to add some information that can be used to adjust for the waveform properties of the interference signal. In this paper we suggest a simple correction factor for the average-power approach. This makes it possible to make a rough adjustment for the interference-waveform properties so that the measured total interference power can be used as a decision metric in future applications. Some of the most important conclusions in the previous sections are listed below.

- Since intersystem interference can affect an ad hoc network in different ways it is important to perform network simulations were the intersystem interference is incorporated.
- If only the interference power is used for determination of the BEP on a communication link, the error in estimated BEP for that link can be in the order of a factor 10000. The largest errors occur if the interference signal consists of pulsed interference.
- The uncertainty of the availability of the SA service in the network analyzed is less than 10% units if the corresponding error in SIR at the node level is less than approximately 2-3 dB.
- By the use of the impulsiveness correction factor, the uncertainty in corresponding SIR can be brought down to below approximately 3 dB for pulsed interference signals which means that the Gaussian approximation can be used as a basis for the interference analyses at the node level.
- OPNET Modeler can be used as a possible simulation environment for intersystem-interference analyses if the Gaussian approximation can be used for interference modeling at node level.
- The results in this report confirm the reported effects in Linder et al. (2004) [16], that even for low data rates and levels of interference that affect all vehicles, there are situations where the battalion commander may not be able to control the companies. The effects are particularly disturbing for direct support of company commanders where a few companies may have large deviations for several minutes.

8 Suggested Topics for Future Work

Based on the conclusions in this report, the following topics are suggested for future work:

- Further investigation of how uncertainties in the node/link modeling affect the conclusions drawn on the network level.
- Further investigation of the possibilities/limits of the ICF for mixed signals.
- Further investigation of how the ICF behaves for systems using forward error-correcting codes.
- Development of a reduced intersystem-interference model in OPNET Modeler.
- While the results indicate that higher levels of intersystem interference may reduce the battalion commanders' situation awareness and trust in the positioning service, these results need to be validated by asking subject matter experts for subjective ratings of how they experience the positioning services on an appropriate scale of trust.

9 References

[1] 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.

[2] *Establishment of an Interference Temperature Metric to Quantify and Manage Interference and to Expand Available Unlicensed Operation in Certain Fixed, Mobile and Satellite Frequency Bands*, FCC document ET Docket No. 03-237, August 13, 2004

[3] Manfred Stecher, "Weighting of disturbance according to its effect on digital radio systems," in *Proc. IEEE International Symposium on Electromagnetic Compatibility*, Denver, CO, 1998, pp. 69-73.

[4] Peter F. Stenumgaard, "A Possible Concept of How Present Radiated Emission Standards Could be Amended in Order to Protect Digital Communication Services" *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, pp. 635-640, November 2004.

[5] Peter F. Stenumgaard, "Using the Root-Mean-Square detector for weighting of disturbances according to its effect on digital communication services" *IEEE Transactions on Electromagnetic Compatibility*, vol. 42, pp. 368-375, November 2000.

[6] ITU DOCUMENT "THE PROTECTION OF SAFETY SERVICES FROM UNWANTED EMISSIONS", AMCP WGF/6 WP/6, Document 1/13-E, 30 October 2000.

[7] Simon Haykin, ”Cognitive Radio: Brain-Empowered Wireless Communications”,IEEE *Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, February 2005.

[8] Stephen Berger et al,” A New Challenge for EMC: Policy Defined Radio”, *IEEE EMC Society Newsletter*, No. 204, pp. 42, Winter 2005.

[9] Peter Stenumgaard, Leif Junholm, “Higher-Order Effects of Radiated Interference - Future Challenging Research Domains within EMC in Dynamic Wireless Communication Networks”, EMC 2005 Zürich, 14-17 February 2005.

[10] Ulf Sterner, Sara Linder, “Effects of Intersystem Interference on a Situation Awareness Service in a Mobile Ad Hoc Network”, RVK 05, Linköping, 14-16 juni 2005.

[11] Ulf Sterner, Sara Linder, “Intersystem Interference in mobile ad hoc networks”, will appear at EMC Europe 2005, Rome, 9-21 September 2005.

[12] Leif Junholm, Peter Stenumgaard, ” Higher-Order Effects of Radiated Interference - Future Challenging Research Domains within EMC in Dynamic Wireless Communication Networks”, will appear at EMC Europe 2005, Rome, September 2005.

[13] Peter Stenumgaard, Leif Junholm, “Higher-Order Effects of Radiated Interference - Challenging Research Domains within EMC in Future Military Dynamic Wireless Communication Networks”, MILCOM 2005

[14] Peter Svenmarck, Ulf Sterner, “Telekonfliktpåverkan på Gemensam Lägesbild”, Emergencies & Public Safety, 18-19 januari 2006.

[15] Sara Linder, Ulf Sterner, “Effects of Intersystem Interference in Mobile Ad Hoc Networks”, EMC Europe 2006, Barcelona(?)

[16] Sara Linder, Peter Stenumgaard, Ulf Sterner, Peter Svenmarck “Intersystem Interference Risks in the Future Swedish Defence”, FOI-R--1405—SE, December 2004, ISSN 1650-1942

[17] D. B. Geselowitz, ”Response of Ideal Noise Meter to Continuous Sine Wave, Recurrent Pulses, and Random Noise, ” *IRE Transactions on Radio Frequency Disturbance*, May 1961.

[18] Ulf Sterner, Karin Dyberg-Rosenqvist, ”Realiserbarhetsstudie - OPNET i framtida telekonfliktverktyg”, FOI Memo 1374, 2005-06-20 (In Swedish)

[19] IEC CISPR 16-1/1999-10: Specification of radio disturbance and immunity measuring apparatus and methods. Part1: radio *disturbance and immunity measuring apparatus.*

[20] 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. Linköping, Sweden: Swedish Defence Research Establishment.

[21] Alvå, P., & Palmqvist, U. (2003). *Battle management support systems in NCW - Scenario*. FOI-R--1030--SE (Swedish). Linköping, Sweden: Swedish Defence Research Institute.

[22] Andersson, J., Malm, M., & Thurén, J. (2003). *System trust*. FOI-R--1121--SE (Swedish). Linköping, Sweden: Swedish Defence Research Agency.

[23] Bickerstaff, P., Phocas, M., & Haddrell, T. (2005, March). The Enemy Inside – GPS Jammed by Room, Host, Self. *GPS World*, (pp. 33-39).

[24] Dedes, G., & Dempster, A. G. (2005). Indoor GPS positioning: Challenges and opportunities. IEEE 62nd Semi-annual Vehicular Technology Conference, September 25-28, Dallas.

[25] Endsley, M. R. (2005). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32-64.

[26] Fogel, A., Helgegren, S., Larsson, A., Lindgren, I., Tomic, S., & Wedin, S. (2004). *BA rescue - a task analysis*. Report FOI-R--1361--SE (Swedish). Linköping, Sweden: Swedish Defence Research Agency.

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

[28] Fransson, J., Albinsson, P.-A., Stjernberger, J., & Axelsson, M. (2002). *Usability evaluation of FUM SLB regarding time-critical command and control*. FOI-R--0677--SE (Swedish). Linköping, Sweden: Swedish Defence Research Agency.

[29] Lee, J. D., & See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors*, 46(1), 50-80.

[30] Lindgren, I., Perggren, P., Jander, H., & Hirsch, R. (2004). *Communication and team performance in BA teams*. Report FOI-R--1507--SE. Linköping, Sweden: Swedish Defence Research Agency.

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

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

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

[34] Thurén, R., Andersson, J., & Svenmarck, P. (2005). *Systemtilltro och tilltro i nätverk – kort slutrapport om en strategisk forskningskärna*. FOI memo, Linköping, Sweden: Swedish Defence Research Agency.

[35] van Diggelen, F., & Abraham, C. (2001, September). Indoor GPS: The no-chip challenge. *GPS World*, (pp. 50-57).

[36] Wilson, J., Steingart, D., Romero, R., Reynolds, J., Mellers, E., Redfern, A., Lim, L., Watts, W., Patton, C., Baker, J., & Wright, P. (2005). Design of monocular head-mounted displays for increased indoor fire fighting safety and efficiency. In Proceedings of the SPIE, Vol. 5800, P. Tchoryk & B. Holz (Eds.), *Spaceborne Sensors II*, (pp. 103-114).

[37] 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.

[38] 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.

[39] 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.

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

[41] 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.

[42] R. K. Ahuja, T. L. Magnanti and J. B. Orlin, *Network Flows. Theory, algorithms, and applications.* Prentice Hall, 1993.

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

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

[45] P. 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.