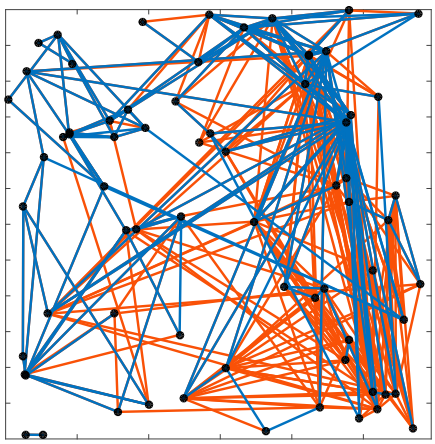
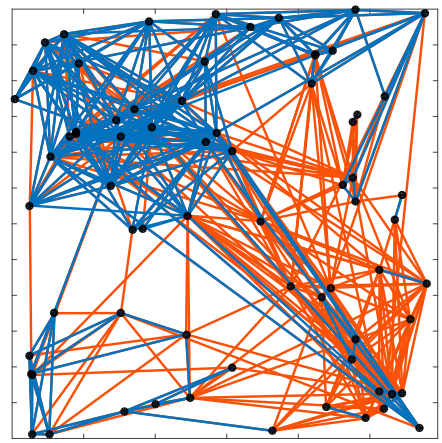
Jamming effects on frequency-hopping ad hoc networks

Performance analysis

ANDERS HANSSON, JAN NILSSON, ULRIKA UPPMAN, ULF STERNER





FOI-R--4222--SE
ISSN 1650-1942 January 2016

Anders Hansson, Jan Nilsson, Ulrika Uppman, Ulf Sterner

Jamming effects on frequency-hopping ad hoc networks

Performance analysis

Titel	Påverkan på frekvenshoppande ad hoc-nät på grund av aktiv störning – Prestandaanalys
Title	Jamming effects on frequency-hopping ad hoc networks – Performance analysis
Rapportnr / Report No.	FOI-R--4222--SE
Månad / Month	Januari / January
Utgivningsår / Year	2016
Antal sidor / Pages	35
ISSN	1650-1942
Kund / Customer	FMV
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT område	Ledning och MSI
Projektnr / Project No.	E324533
Godkänd av / Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Abstract

Protection against jamming is essential for tactical radio networks. Frequency hopping (FH) is an often used jamming protection technique. An adaptive jammer, such as a fast follower jammer can be a serious threat to a tactical ad hoc network using FH. Another non-adaptive FH jamming threat is partial-band noise jamming.
In this report, ad hoc networks exposed to jamming are examined. Firstly, an approximative analytical method and performance criteria are devised. Using these criteria for follower and partial-band jamming we examine the effect of parameters like distance to jammer, communication distance between nodes, frequency hopping rate, jamming power, response time of jammer and error correcting capability of the radio system. Secondly, to study network properties under follower jamming, network simulations are performed. Focus is to examine how the terrain and the network protocols influence the jamming resistance. The terrain influences how easy it is to jam a network. For the cases investigated, a network in a flat terrain becomes more jammed than the corresponding network in a hilly terrain. The packet delivery ratio is measured when the network protocol OLSR MPR-flooding is used and compared to a network using full flooding. Even if not as robust as full flooding, OLSR MPR-flooding is still relatively robust. We also show that it is enough to jam the control slots used by the network protocols to have an impact on the network delivery ratio.

Keywords: Ad hoc networks, follower jammer, partial-band jammer, OLSR MPR-flooding, terrain effects

Sammanfattning

För ett taktiskt radionät är det viktigt med ett skydd mot aktiv störning. En ofta använd skyddsmetod är frekvenshopp (FH). En adaptiv störare som en snabb följestörare kan dock vara ett allvarligt hot mot att ad hoc-nät som använder FH. Ett annat, icke-adaptivt störhot mot FH system är delbandsstörning.
I denna rapport undersöks ad hoc-nät utsatta för aktiv störning. Först tas en approximativ analytisk metod fram tillsammans med ett antal prestandakriterier. Med hjälp av dessa kriterier undersöks hur störningen påverkas av parametrar såsom avstånd till störare, kommunikationsavstånd mellan noder, frekvenshopptakt, störarens effekt, störarens svarstid och felrättningsförmåga hos radiosystemet. Därefter undersöks nätets egenskaper då det är utsatt för störning med hjälp av nätsimuleringar. Fokus ligger på att undersöka hur terrängen och nätprotokollen påverkar nätet vid följestörning. Terrängen påverkar hur enkelt det är att störa ett nät. I de undersökta fallen blir nätet i den platta terrängen mera utstört än det motsvarande nätet i den kuperade terrängen. Paketfelhalten används som prestandamått och jämförs för ett nät där nätverksprotokollet OLSR MPR-flödning används med ett nät som använder full-flödning. OLSR MPR-flödning är relativt robust vid störning, men inte lika robust som full-flödning. Vi visar också att det är tillräckligt att endast störa protokollkontrolltrafiken för att påverka paketfelhalten.

Nyckelord: Ad hoc-nät, följestörning, delbandstörning, OLSR MPR-flödning, terrängpåverkan

Contents

1 Introduction

A common threat to military radio and tactical networks is deliberate jamming. A radio system can be made more or less robust against jamming. However, to protect a radio network against jamming has a cost in terms of reduced capacity. Frequency hopping (FH) is an often used jamming protection technique, as transmitting FH signals over large bandwidths is fairly easy. A fast follower jammer can be a serious threat to a tactical ad hoc network. The threat can be regarded as increasing, as very capable real-time spectrum analyzers and waveform generators are commercially available and fast follower jammers can be built based on such commercial equipment. In an earlier work [1, 2] we analyzed frequency hopping system using random dwell-time to increase the resistance to jamming.

Another, non-adaptive, FH jamming threat is partial-band noise jamming. The partial-band noise jammer concentrates jamming power in a fraction of the system bandwidth. The FH system can therefore not mitigate the effect of the partial-band noise jammer by increasing the hop rate. On the other hand, the partial-band jammer has a power disadvantage compared to the follower jammer. An ad hoc network is a radio network without any centralized node, where transmitted packets can be relayed via other nodes. Relaying makes it somewhat robust to jamming due to rerouting via unjammed links.

In this report, to study ad hoc networks exposed to jamming we use two approaches. In the first approach we devise an approximative analytical method together with relevant performance criteria. These criteria make it possible to study many different jamming scenarios and deduce generic results. Typical questions include, is the hopping rate sufficient to protect the network, or is a particular jammer at a given distance a threat, etc. Moreover, the sensitivity of the parameters of the radio system and the jammer can easily be analyzed. In the second approach event based network simulations are performed. Then, more detailed results of the network performance can be obtained. We use radio network routing protocol implementations and terrain based channel models. In a jamming scenario, we show how the jamming vulnerability differs between terrain types. We also study the robustness of the routing protocol OLSR MPR-flooding and show the effects of intelligent jamming taking advantage of the routing protocol structure. A motivation for our work is that protection against a jammer is an important issue for tactical radio network performance.

In the presented assessment generic radio parameters are used and the performance of the jammer is based on what can be obtained with commercial equipment constituted by, for example, a spectrum analyzer and a signal generator.

Traditionally, spread-spectrum systems including frequency-hopping systems and their jamming protection are extensively studied in the literature, e.g., in [3]. How high a reasonable hopping rates can be for combat radios are examined in [4].

The report is organized as follows: Chapter 2 analyzes how the communication links in ad hoc networks are affected by a follower jammer and a partial-band jammer. The analysis utilizes a approximative analytical method to calculate performance criteria. In Chapter 3, network simulations are used to study effects on frequency-hopping ad hoc networks due to following jamming. Of particular interest is how the network

protocols and the terrain influence the jamming resistance. Finally, the conclusions are presented in Chapter 4.

2 The effect of jamming for different technical scenarios

In this chapter we perform an analysis of how ad hoc networks are affected by a follower jammer and a partial-band jammer. Moreover, an approximative analytical method and performance criteria to analyse the effect are described. We start with the critera for the follower jammer, then in 2.1.5 the criteria for the partial-band jammer is described.

2.1 Analytical method

It is assumed that the follower jammer performs the detection and jamming in sequence. The conditions for a follower jammer to successfully jam a frequency-hopping ad hoc network can be summarized by the three criteria:

1. Detection of a signal transmitted by a node in the ad hoc network at a certain frequency.
2. Sufficient jamming power must reach the receiving nodes in the ad hoc network.
3. The jamming signal must reach the receiver sufficiently in time before the frequency is changed.

Criterion 1 is determined by the ability of the jammer to detect a radio signal. For the analysis we assume that the jammer is able in the detection phase to incorporate the entire frequency band the ad hoc network is using. Criterion 2 is determined by the received jamming power in relation to the received signal power. This means that the distances between the jammer and radio receivers, and the distances between the transmitter and radio receivers are crucial. Both criterion 1 and 2 are strongly influenced by the wave propagation in the adopted scenario. Criterion 3 involves the frequency-hopping rate of the ad hoc network in relation to the distance between transmitter, receiver and jammer. For the follower jammer to succeed, all three criteria need to be met.

2.1.1 Communication distance

For any link in the radio network, the signal-to-noise ratio at a receiver needs to exceed a certain threshold level τ_1,

$$\frac{E_b}{N_0} = \frac{P_T G_T G_R}{L_{TR} R k T_0 F} > \tau_1. \tag{2.1}$$

In this relation, E_b denotes the bit energy and N_0 is the single-sided spectral density of the thermal receiver noise. Furthermore, P_T is the transmitter power, G_T and G_R are the transmitter and receiver antenna gain, R is the data rate, k is the Boltzmann constant, and F is the system noise factor relative a reference thermal noise source with

temperature $T_0 = 290K$. To calculate the link attenuation L_{TR} for the communication distance r_{TR}, the two-ray ground model for the wave propagation is used,

$$L_{TR} = \frac{r_{TR}^4}{(h_T h_R)^2,} \tag{2.2}$$

where h_T and h_R are the transmitter and the receiver antenna heights. Hence for the link to be functional, it needs to fulfill the following relation

$$r_{TR} < \frac{P_T G_T G_R}{RkT_0F} \frac{(h_T h_R)^2}{\tau_1}.$$

2.1.2 Detection distance for the jammer

In the analysis, the receiver sensitivity of the jammer is assumed to be -155 dBm/Hz. The value -155 dBm/Hz is a typical value for a spectrum analyzer [5]. By assuming that the detection threshold is approximately equal to the receiver sensitivity level, the jammer will have a detection level of -105 dBm for a receiver bandwidth of 100 kHz. For the jammer to detect the transmitted signal, the following relation needs to be fulfilled

$$\frac{P_T G_T G_J}{L_{TJ}} > 10^{-(105+30)/10},$$

where G_J is the jammer antenna gain in the current direction and L_{TJ} is the attenuation between the transmitter and the jammer. As for the communication path loss, the attenuation between the transmitter and the jammer is calculated with the two-ray path-loss model given in Equation 2.2,

$$L_{TJ} = \frac{r_{TJ}^4}{(h_T h_J)^2}, \tag{2.3}$$

where h_J is the jammer antenna height and r_{TJ} is the distance between the transmitter and the jammer. The maximum detection distance can then be derived as

$$r_{TJ} < (10^{\frac{105+30}{10}} P_T G_T G_J (h_T h_J)^2)^{\frac{1}{4}}.$$

2.1.3 Jamming distance due to power advantage

When the jammer has detected a signal, the jammer will, after the response time T_r, output the jamming power on the current frequency. As in the requirement for communication distance 2.1, we assume that the energy per information bit is $E_b = \frac{P_T G_T G_R}{R L_{TR}}$, and the noise in the reciver without jamming is modeled as white gaussian noise with power spectral density $N_0 = kT_0F$. We model the jamming signal in the receiver as gaussian noise with power spectral density $\widetilde{N}_0 = \frac{P_J G_J G_R}{L_{JR} W}$ (W/Hz), where W is the instantaneous bandwitdth for the communication system and L_{JR} is the attenuation between the jammer and the receiver. We assume that a jammed link in the radio

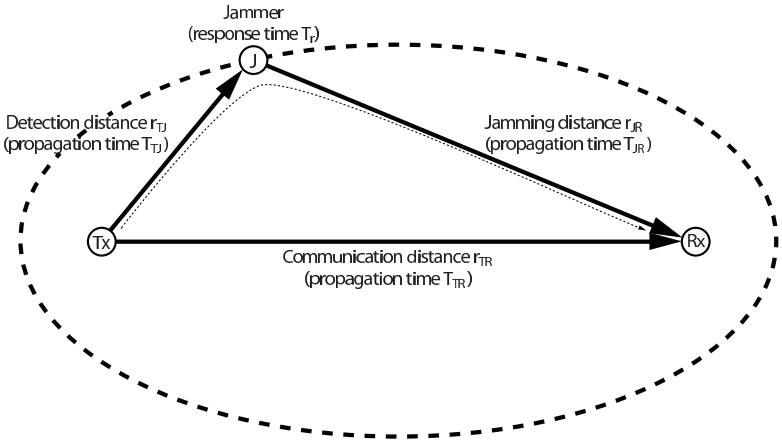


Figure 2.1: Follower jamming distances.

network can be used for communication if the signal-to-noise-and-interference ratio (SINR) at a receiver exceed a certain threshold level τ_2:

$$\frac{E_b}{\widetilde{N}_0 + N_0} = \frac{\frac{P_T G_T G_R}{R L_{TR}}}{\frac{P_J G_J G_R}{L_{JR} W} + kT_0 F} > \tau_2 \tag{2.4}$$

In Equation 2.4, L_{JR} is calculated with the two-ray path-loss model given in Equation 2.2,

$$L_{JR} = \frac{r_{JR}^4}{(h_J h_R)^2}, \tag{2.5}$$

where r_{JR} is the distance between the jammer and the receiver. Hence, for sufficient jamming power to reach the receiver, the power advantage criteria for distance r_{JR} can be calculated by first solving L_{JR} from equation 2.4:

$$L_{JR} < \frac{P_J G_J G_R}{kT_0 F} \left(\frac{1}{1 - \frac{L_{TR}}{\frac{P_T G_T G_R}{\tau_2 R k T_0 F}}} - 1\right) \tag{2.6}$$

where L_{TR} is given by 2.2 and r_{JR} is solved from Equation 2.5 :

$$r_{JR} < L_{JR}^{1/4} (h_J h_R)^{1/2}.$$

2.1.4 Timing criteria for FH with fixed dwell time

In addition to the previous conditions, the jamming power at a certain frequency must reach the receiver before the radio signal at the receiver has switched frequency. The time on each frequency is denoted the dwell time of the frequency hopping system, T_{dw}. In Figure 2.1, we can see the classical illustration of a follower jammer and a transmitter and a receiver [4]. The figure shows the distances between the transmitter,

jammer and the receiver. The corresponding propagation time is also included in the figure; T_{TR} denotes the propagation time between the transmitter and the receiver, T_{TJ} is the propagation time between the transmitter and the jammer and T_{JR} is the propagation time between the jammer and the receiver.

We assume that the follower jammer initially is in its detection mode. As the follower jammer is reached by transmitted power, it takes a response time, T_r, to output interference power on the particular frequency. The follower jammer is then interfering the rest of the frequency hop. Due to the different propagation times, the jamming power will begin to affect the received signal a time $T_{TJ} + T_{JR} - T_{TR} + T_r$ after the signal from the receiver is received, see Figure 2.1. If the jammer disturbs a sufficient part of the dwell-time, the error correction capability of the radio system cannot take care of the errors and the jammer will succeed. Let us assume that the radio system can withstand at most ρ of the dwell time to be disturbed. Then, the jammer needs to jam more than a fraction ρ of the dwell time for successful jamming, or equivalently, the following relation has to be fulfilled,

$$T_{TJ} + T_{JR} - T_{TR} + T_r < T_{dw}(1 - \rho). \tag{2.7}$$

2.1.5 Partial-band jammer

One intelligent, but non-adaptive FH jamming threat is partial-band noise jamming. The partial-band noise jammer concentrates jamming power in a fraction of the system bandwidth. In practice, the jammer may also hop the noise band to prevent avoidance countermeasure, i.e., the FH system detects which band that is jammed and avoid using it.

We let c denote the number of available channels for the radio system. The system bandwidth then becomes cW, where W is the instantaneous bandwidth. This system bandwidth may be spread out in a noncontiguous frequency band. Finding a large enough available contiguous frequency band can be difficult. Another reason to chose a noncontiguous frequency band is to make it more difficult for the partial-band jammer. However, we do not take this into account in our analysis and consider a contiguous frequency band.

The follower jammer needs to jam at least ρ of the dwell time to be successful. The analogy for the partial-band jammer is that at least ρ of the system bandwidth cW has to be jammed. In 2.1.3, the power criteria for the follower jammer is described. For the partial-band jammer the power criteria is obtained in similar way, by inserting the jammed bandwidth $cW\rho$ instead of W in Equation 2.4:

$$\frac{E_b}{\widetilde{N}_0 + N_0} = \frac{\frac{P_T G_T G_R}{R L_{TR}}}{\frac{P_J G_J G_R}{L_{JR} cW\rho} + kT_0F} > \tau_2 \tag{2.8}$$

2.1.6 Approximative analytical method

In this section we introduce the approximative method, that simplifies the previous analysis, by reducing the number of distances involved. The previous analysis involves

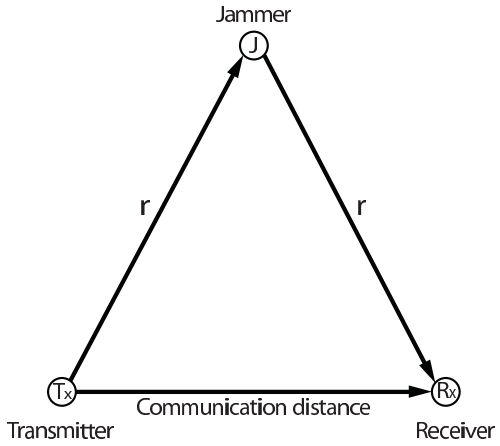


Figure 2.2: Simplified analysis

three distances r_{TJ}, r_{JR} and r_{TR}, meaning that each communication link in the network is affected, at least slightly, differently by the jammer. A way to simplify the analysis is to assume an equal jammer distance r to the the transmitter and the receiver. That is, in the equations we set $r_{TJ} = r_{JR} = r$, $T_{TJ} = T_{JR} = T$, and $L_{TJ} = L_{JR}$. The topology becomes as shown in Figure 2.2. Then we can calculate for the different criteria how the communication distance r_{TR} depends on the distance to the jammer r.

2.2 System and parameters

The effect of jamming depend on the communication and jamming system as well as the location of the jammer and the topology of the network. However, in this and the next section the approximative analysis is used. This means that we do not specify a whole network, only the communication distance between the nodes are included in the analysis. Important parameters are distance to jammer, communication distance, jamming power, response time of jammer and correcting capability of the radio system.

Both a NarrowBand-WaveForm (NBWF) and a WideBand-WaveForm (WBWF) system are investigated. The instantaneous bandwidth is 50 kHz and 1 MHz for the NBWF and the WBWF system, respectively. The radio system can withstand at most ρ of the dwell time to be disturbed, see 2.1.4.

The parameter ρ can be seen as the erasure correcting capability of the system. An erasure is a received bit that can be identified as unreliable and is erased. Therefore it can more easily be corrected than a random bit error. We are interested in high, medium and low code rate system and investigate the three following values for ρ: 0.2, 0.33, 0.5. The parameters of the radio systems are given in Table 2.1.

We consider two types of jammers, called a strong and a weak jammer. The strong jammer is a capable jammer with 1000 W output power and an antenna elevation height of 24 meter. The weak jammer has output power 50 W and an antenna elevation height of 6 meter, the parameters of the jammer are given in Table 2.2. It is assumed that

the weak jammer is more mobile than the strong jammer, it can stop at a location, quickly get ready to jam for a short while, and then move on to another location. As a consequence it is anticipated that the weak jammer will be able to operate closer to the network. The response time of the jammer is important, and it is assumed that the response time can be shorter for a wide-band system than for a narrow-band system. Therefore in the evaluation we use the response times 25 μs and 100 μs for WBWF and 100 μs and 500 μs for NBWF. Furthermore, it is assumed the jammer only can operate with a limited antenna gain as it has to be able to jam a rather wide sector (between 60 to 90 degrees) to cover the whole ad hoc network. We have fixed the antenna gain to 8 dB even if the antenna gain of the jammer in practice could be adapted to the situation, the distance to the network and the estimated maximum communication distance between nodes.

Partial-band jamming is also considered. In that case it is the available system bandwidth cW in relation to the instantaneous bandwidth of the radio system that is important. We assume that the number of channels c can be much larger for the NBWF system than for the WBWF system (500 instead of 10).

Table 2.1: Parameters of communication nodes.

Parameter	NBWF	WBWF
Hop rate	1 hop/ms, 2 hop/ms	1 hop/ms, 4 hop/ms
Output power, P_T	20 W	40 W
Signal bandwidth, W	50 kHz	1 MHz
System bandwidth, cW	25 MHz	10 MHz
Antenna gain, G_T, G_R	0 dB	0 dB
Antenna elevation height, h_T, h_R	3 m	3 m
SNR-threshhold, τ_2	7 dB	7 dB
Datarate, R	20 kbit/s	1 Mbit/s
Erasure correcting capability, ρ	0.20 , 0.33, 0.50	0.20 , 0.33, 0.50
Noise factor, F	20 dB	20 dB

Table 2.2: Parameters of jammer.

Parameter	weak jammer	strong jammer
Output power, P_J	50 W	1000 W
Antenna gain, G_J	8 dB	8 dB
Antenna elevation height, h_J	6 m	24 m
Response time (NBWF), T_r	100 μs,500 μs	100 μs,500 μs
Response time (WBWF), T_r	25 μs, 100 μs	25 μs, 100 μs
Detection sensitivity	-105 dBm	-105 dBm

2.3 Results

In this section we use the approximative analytical method for jamming evaluation, described in 2.1.6, and study the impact of the three criteria mentioned in section 2.1 that limits the range of a jammer. The parameters for the investigated communication and jamming systems are presented in section 2.2.

The time criteria depends on distances, frequency hopping rate, erasure correcting capability ρ, and response time T_r. It shows that an increased hop rate improves the resistance to follower jamming. This happens if the time criteria limits the jammers range. Clearly, the follower jammer needs to be closer than the detection distance to be able to detect the signal at all and determine which frequency to jam. The jammer also need to be closer than the distance given by the power criteria otherwise the jamming power is insufficient.

Figures 2.3 to 2.10 show one diagram for each combination of the four parameter options: weak or strong jammer, slow or fast jammer, low or high hop rate, NBWF or WBWF, described in section 2.2. We compare the three criterias for follower jamming to the power criteria for the partial-band jammer. Note that the erasure correction capability ρ is set to 0.3 for the partial-band jammer case in all the figures. When comparing power criteria the partial-band jammer will always have a power disadvantage and has to be closer to the network than the follower jammer to be able to jam a link of a given length.

For example consider the NBWF system with a hop rate of 1 hop/ms jammed by the weak jammer in Figure 2.3. The detection distance is about 33 km and the time criteria give minimum distances to jammer larger than 60 km. Thus, the hopping rate is not sufficient high in this case the improve the jamming resistance. The follower jammer needs to be closer than 33 km to the network to jam 10 km and longer communication link, and closer than about 17 km to the network to jam 5 km and longer communication links. In this case, the partial-band jammer is inferior and needs to be closer than 10 km to the network to jam 10 km and longer communication links, and closer than about 5 km to the network to jam 5 km and longer communication links.

As an other example consider the WBWF system with a hop rate of 4 hop/ms jammed by the strong jammer in Figure 2.10. In this case the detection distance is sufficiently large due to a much higher elevated antenna and 40 W transmit power instead of 20 W for the communication system. The follower jammer has sufficient power to jam communication links 2.7 km and longer at a distance 40 km away. However, the time criterion forces the follower jammer to be much closer to the network to jam such links, e.g., at most 11 km away if $\rho = 0.3$ and at most 5 km away if $\rho = 0.5$. In this case, it is better to use the partial-band jammer; it can jam communication links 2.7 km and longer at a distance 30 km away.

The results show that a large available bandwidth makes partial-band jamming difficult. The partial-band jammer is rather competitive, when compared to the follower jammer for WBWF ($c = 10$), but inferior the follower jammer for NBWF ($c = 500$). Follower jamming is preferable for the fast jammer case (response time 100 μs) against NBWF, see Figure 2.3 and 2.5. The time criteria is critical for the slow (response time 500 μs) follower jammer performance aganist NBWF with low hop rate, see Figure 2.4 and 2.6 . Here the erasure correction capability decides wether follower jamming

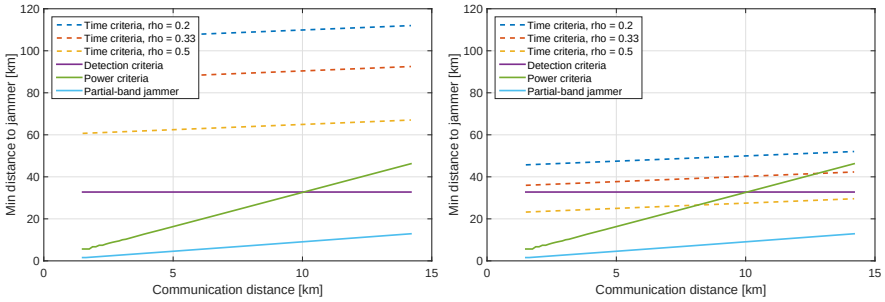


Figure 2.3: NBWF, weak jammer with response time $t_r = 100\mu$s, hop rate 1 hop/ms (left) and hop rate 2 hop/ms (right).

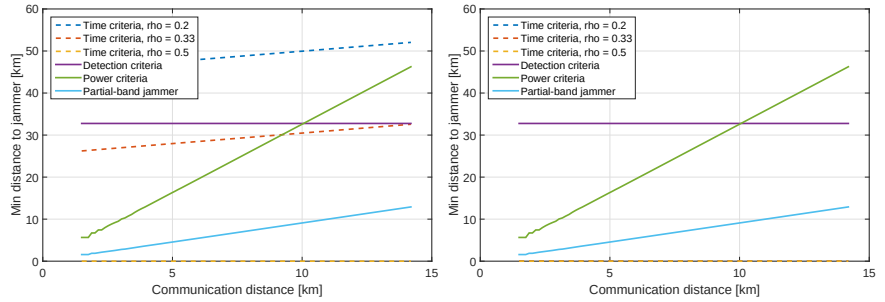


Figure 2.4: NBWF, weak jammer with response time $t_r = 500\mu$s, hop rate 1 hop/ms (left) and hop rate 2 hop/ms (right).

or partial-band jamming is preferable. For the high hop rate (2 hop/ms) for NBWF, the time criteria makes follower jamming useless and the partial-band jammer must be used. Since partial-band jamming is less expensive and less complex compared to follower jamming, it is a better choice when the jamming performance is comparable between the two methods. So for jamming with the weak jammer against WBWF, we note that partial-band jamming is preferable because the difference in the power criteria is quite small between the partial-band jammer and the follower jammer, see Figure 2.7 and 2.8. For jamming with the strong jammer against WBWF, there is a larger difference in the power criteria between the partial-band jammer and the follower jammer. For example, with a communication distance of 4 km, the follower jammer can be 15 km further away from the communication nodes than the partial-band jammer. Follower jamming is preferable for the slow hop rate (1 hop/ms). For the high hop rate (4 hop/ms), the time criteria dominates and makes the follower jamming range small compared to partial-band jamming. Therefore partial-band jamming is preferable, see Figures 2.9 and 2.10.

How the hop rate influences the time criteria at a communication distance of 8 km is shown Figure 2.11. The time criteria are calculated for hop rates up to 8 hop/ms and are valid for both types of communication and jamming system. However, this criteria may not be the limiting one. Note, the minimum distances to jammer can not be smaller

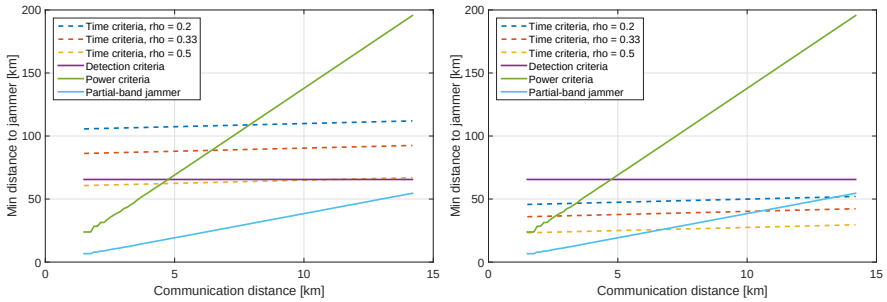


Figure 2.5: NBWF, strong jammer with response time $t_r = 100\mu$s, hop rate 1 hop/ms (left) and hop rate 2 hop/ms (right).

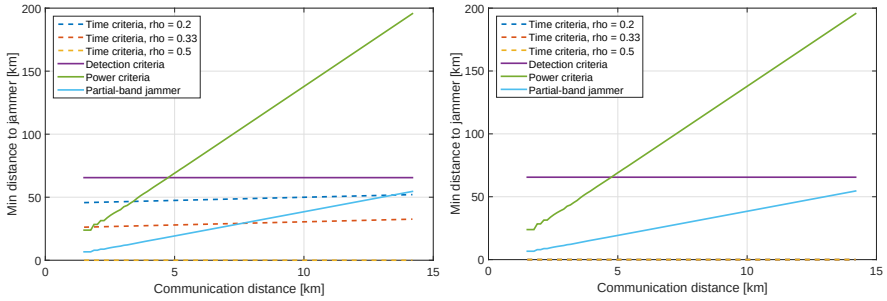


Figure 2.6: NBWF, strong jammer with response time $t_r = 500\mu$s, hop rate 1 hop/ms (left) and hop rate 2 hop/ms (right).

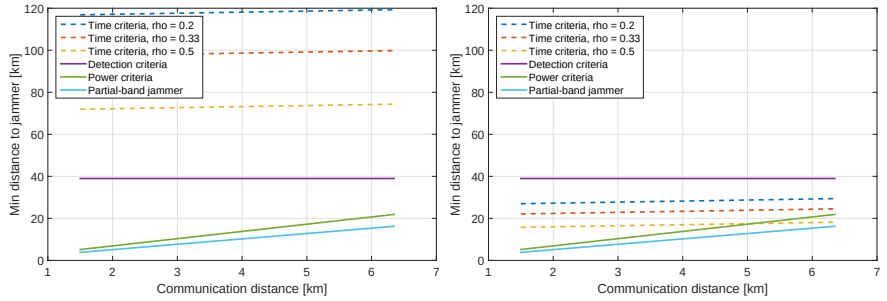


Figure 2.7: WBWF, weak jammer with response time $t_r = 25\mu$s, hop rate 1 hop/ms (left) and hop rate 4 hop/ms (right).

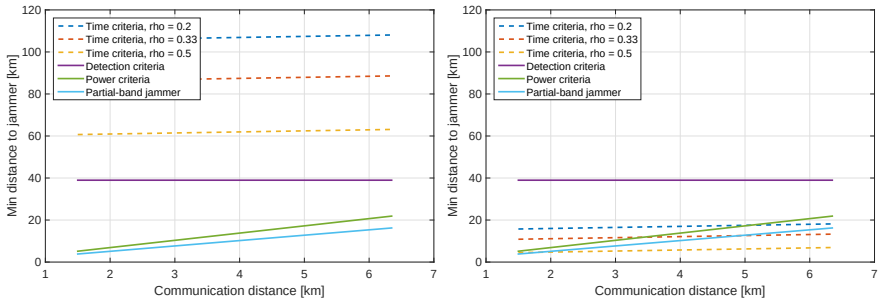


Figure 2.8: WBWF, weak jammer with response time $t_r = 100\mu$s, hop rate 1 hop/ms (left) and hop rate 4 hop/ms (right).

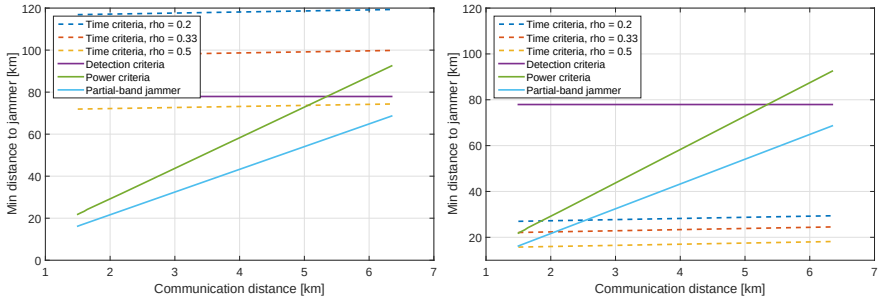


Figure 2.9: WBWF, strong jammer with response time $t_r = 25\mu$s, hop rate 1 hop/ms (left) and hop rate 4 hop/ms (right).

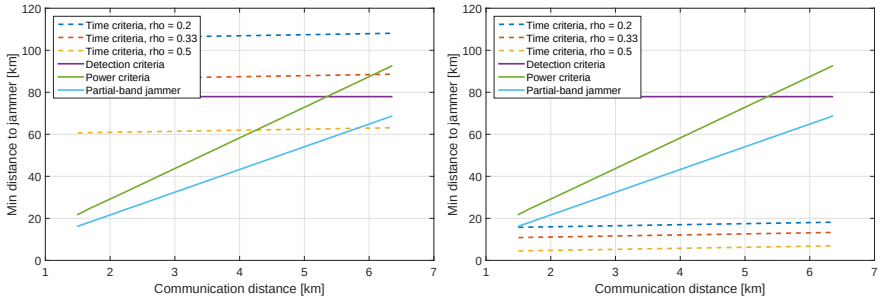


Figure 2.10: WBWF, strong jammer with response time $t_r = 100\mu$s, hop rate 1 hop/ms (left) and hop rate 4 hop/ms (right).

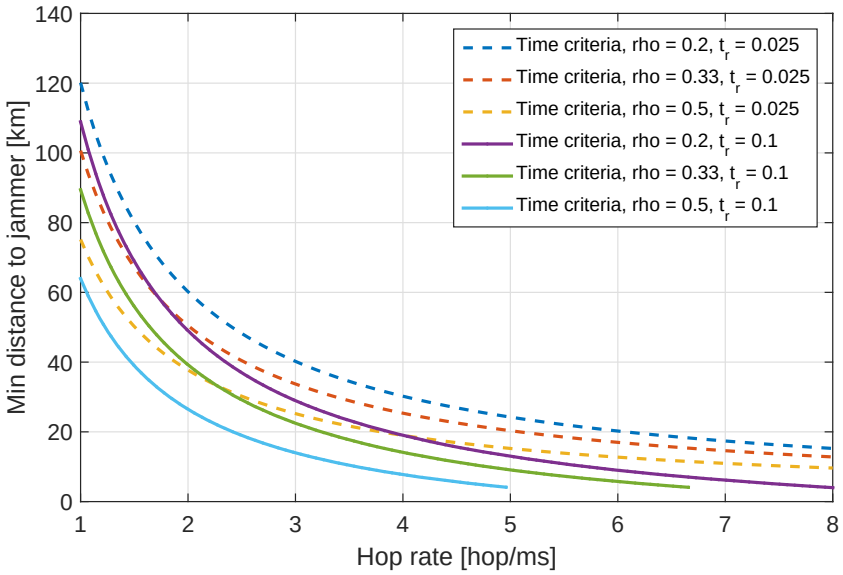


Figure 2.11: Communication distance $r_{TR} = 8$ km.

than 4 km, when the jammer is placed in between the transmitter and the receiver, as the communication distance is 8 km. As can be seen, rather high hopping rates are required to force the follower jammer close to the network. To force the jammer closer than 15 km a hop rate of at least 3 hop/ms is required, also with the robust low rate system ($\rho = 0.5$) and the slower jammer ($t_r = 0.1$). In case of the fast jammer, hop rates above 5-6 hop/ms are required. If a fast jammer gets closer very high hopping rates are required to protect the network. In [2] we showed that a hopping rate of about 10-12 hop/ms is required to protect the network if a fast follower jammer is located 5 km from the network.

2.3.1 Result conclusions

Table 2.3 is a summary of the evaluation displayed in figures 2.3 to 2.10. It shows whether follower jamming or partial-band jamming is preferable for the four different jammer cases (in the rows) and the four evaluated communication systems (in the columns). We also indicate when the time criteria is critical for the follower jamming performance. For WBWF, rather high hopping rates are required to protect the network from a follower jammer. However for a mobile jammer with low power, there is little gain for the jammer to choose follower jamming instead of partial-band jamming. Using a high hopping rate does not help much if only a small system bandwidth is available, i.e., few channels to hop between. For NBWF the fast follower jammer, with response time 100 μs, is more efficient than the partial-band jammer.

Table 2.3: Results summary for the different jammer cases (in the four rows) and the evaluated communication systems (in the four columns).

Transceiver→ Jammer↓	NBWF low hop rate	NBWF high hop rate	WBWF low hop rate	WBWF high hop rate
Weak Fast	Follower	Follower	Partial-band	Partial-band
Weak Slow	Time-crit.	Partial-band	Partial-band	Partial-band Time-crit.
Strong Fast	Follower	Follower	Follower	Partial-band
Strong Slow	Time-crit.	Partial-band	Follower	Partial-band

Follower : Follower jamming is preferable for the jammer.
Partial-band : Partial-band jamming is preferable for the jammer.
Time-crit.: Small changes in time criteria affects follower jamming protection.

3 Analysis of jamming effects on routing protocols in different terrains

In this chapter we present results from detailed event based network simulations using radio network routing protocol implementations and terrain based channel models. In a scenario with a follower jammer, we will show how the jamming vulnerability differs between terrain types. We will also show the effects of an intelligent jammer that take advantage of the routing protocol structure, as we look at the possibilities of a follower jammer that is jamming only the control slots of a network using the OLSR protocol with an MPR-flooding routing algorithm.

Two different terrain types are investigated, which are described further in section 3.1. The parameters of the network nodes and the jammer are presented in section 3.2 and 3.3 respectively, and in section 3.4 the simulation environment setup and radio implementation is described further. The results will be presented in section 3.5.

3.1 Terrain and scenario

Simulations are run in two different areas with different terrain type. Firstly, we look at an area in northern Sweden with hilly terrain. Here the hills are steep and the vegetation is typical Swedish forest. Secondly, we look at an area in the south of Sweden where the terrain is more flat. Although the flat terrain still has some hills and vegetation, so it is far from a plane earth model. The channel path gain is pre-calculated for the chosen terrain areas using DetVag-90. For more on DetVag-90, see [6], [7]. As a reference, simulations are also run using the plane earth model where the path gain is calculated as in Equation 2.2 in section 2.1.1.

The communication network nodes are moving around in an area of 12×12 kilometers, in a random walk pattern. The jammer is stationary at a distance of 5 kilometers from the end of the communication network, see Figure 3.1.

To be fair, the jammer would not position itself in a valley or behind an obstacle from the target. We have therefore placed the jammer on a position that is relatively

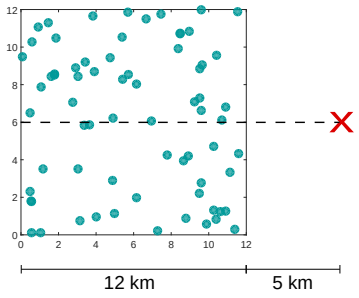
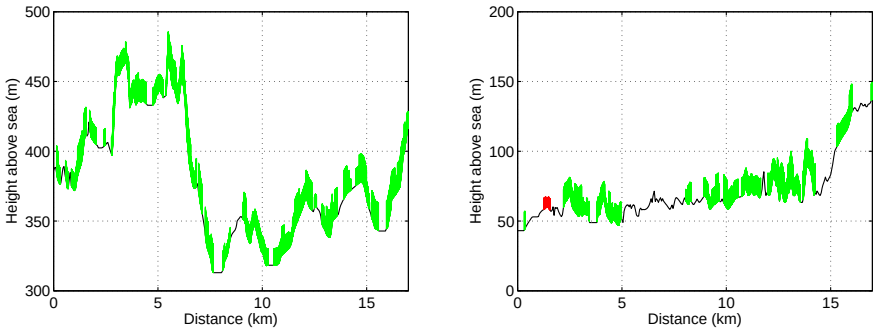


Figure 3.1: 70 network communication nodes are moving inside a square 12×12 km area. The jammer is stationary 5 km east. The dashed line marks the terrain profiles in Figure 3.2.

favourable at least in the direction of the center of the communication network. See Figure 3.2 for terrain profiles between the jammer and the communication network.



(a) Hilly terrain (b) Flat terrain

Figure 3.2: Terrain profiles for the two terrain types. The black line is the ground level, the green is vegetation (trees) and the red is buildings. The terrain profile is taken from the marked line in Figure 3.1. The communication network nodes are located in the area between 0 and 12 km. The jammer is located at 17 km (i.e. 5 km from the end of the network).

3.2 Communication network parameters

The parameters used for each communication node are presented in Table 3.1. The network consists of 70 nodes moving around an area of 12 $\times$ 12 kilometers. The nodes are communicating by sending broadcast traffic in the network, i.e. all packets are sent to all nodes. The amount of traffic in the network is low enough not to overload the network capacity. To investigate the effect on the routing protocol, both OLSR (using MPR-flooding) and a full flooding algorithm are analysed.

Table 3.1: Parameters of communication network nodes.

Parameter	Value used
Output power	40 W
Antenna gain	$\times$1 (0 dB)
Antenna elevation height	3 m
Detection sensitivity	-105 dBm
SNR-threshhold	7 dB
Erasure correction capability	1/3
Datarate	1 Mbit/s
Frequency hop rate	1, 2, 4, 6, 8, 10 khop/s
Noise factor	20 dB
Routing protocol	OLSR, Flooding

For the communication nodes, the frequency hop rate parameter is varied between simulation runs. The frequency hop rate is set so that a single TDMA time slot is split in a number of frequency hops. The hop rates are therefore chosen so that the number of hops per slot is an integer. In our simulations, the data slot length is 2 ms (excluding preamble and guard times). Table 3.2 present the time spent per frequency hop. The frequency hop lengths presented include a short synchronization preamble. In OLSR there are both data and control slots. The control slots are shorter than the data slots, only 1 ms, but the time spent per frequency hop is the same for for both control and data slots for any given hop rate.

Table 3.2: Time per hop for different frequency hop rates.

Hop rate (khop/s)	Time per hop (ms)
1	1.001
2	0.501
4	0.251
6	0.168
8	0.126
10	0.101

3.3 Jammer parameters

In these simulations is a single follower jammer is used. The jammer parameters are presented in Table 3.3. Some of the parameters are varied between the different simulation runs.

Table 3.3: Parameters of jammer.

Parameter	Values used
Output power	50 W, 1000 W
Antenna gain	$\times$8 (9 dB)
Antenna elevation height	6 m
Response time	25 μs, 100 μs
Detection sensitivity	-105 dBm
Distance from net	5 km

The scenario with a jammer at a distance of 5 kilometers from the far end of the network might seem a bit optimistic from the jammer's point of view. However, the terrain made it hard to find suitable jammer positions further away from the communication network. To limit the number of simulations, we chose to use the 5 kilometer jammer distance only. To make the scenario more realistic, we run simulations with a jammer output power of 50 W, to behave like a smaller and more mobile jamming

platform in comparison with the 1000 W output power used as an example of a heavy jammer.

3.4 Simulation framework

For the simulations in this study, our in-house network simulator Aquarius is used. In this study the user traffic is broadcasted in the network using either a full flooding algorithm or MPR-flooding using OLSR.

Aquarius has an OLSR implementation following the standard OLSR RFC 3626 [8]. To increase the robustness of the routes, OLSR includes an optional link hysteresis model that, based on received control packets, tries to estimate the reliability of a link. This hysteresis model is activated in our OLSR simulations. Using the default parameters for the hysteresis algorithm, OLSR will consider a new link reliable if three consecutive control packets are received. However, if one packet is lost on a reliable link, the link will be considered unreliable.

The routing of the packets in the OLSR network is done by the Multi-Point-Relay (MPR) method, most promptly described as the Simplified Multicast Forwarding (SMF) framework [9]. The MPR selection algorithm is described in the OLSR RFC 3626 [8]. At MAC-level, a basic time-division multiple access protocol, with equal static sharing of time slots, is used for all simulations. For a more detailed description of the waveform see [10].

At the physical level of the receiving node, the signal-to-interference level (SINR) per frequency subchannel is recorded per time event basis. The channel capacity per subchannel C_i is calculated according to Equation 3.1.

$$C_i = \min\left(C_{\text{max}}, \log_2\left(1 + \frac{P/\tau}{WN + J}\right)\right) \tag{3.1}$$

Where P is the received signal power per subchannel, τ is SNR margin, W is the subchannel bandwidth, N is the noise spectral density and J is the interference per subchannel. There is also a limitation on the channel capacity, C_{max}, to prevent the capacity to exceed the maximum possible capacity by our specified modulation and coding scheme.

A packet is successfully received if the total channel capacity average over time and frequency of the entire packet arrival, exceeds the threshold C_{th}, as described in Equation 3.2

$$\frac{1}{T_p}\frac{1}{S}\sum_{i=1}^{S}\sum_{j=1}^{M_t} C_i t_j > C_{\text{th}} \tag{3.2}$$

where S is the number of subchannels, T_p is the total packet length, t_j is the time duration over which C_i is constant and M_t is the number of these time intervals.

As an example; in our case we have 1 Mbps datarate and 1 MHz bandwidth which would gives us a capacity threshold, C_{th}, of 1 bit/Hz. This is the threshold to successfully receive a packet. To include the SNR threshold of 7 dB, the SNR margin τ is used. We also have an erasure correction capability of 1/3 which needs to be accounted

for. Therefore the maximum channel capacity limit, $C_{\max}$, is set to 2/3 so that if 1/3 or the packet is lost but the rest of the packet is received without any loss, the packet will still be successfully received.

3.5 Simulation results

Because of the terrain, the position of the jammer is critical. A good position can give the jammer a line of sight to the target even at long distances, but a bad position can block the signal path entirely. These simulation results are to be seen as an example of a possible jammer position, as explained in section 3.1.

The effects of altering the terrain, the output power of the jammer and the response time of the jammer will be presented. All other parameters, positions and movements on the communication network are identical in all simulations. We will also show results on the impact of intelligent jamming of the communication protocol OLSR by only jamming the control slots, in contrary to jamming all data slots. Also the difference between jamming a network running an OLSR protocol that uses MPR-flooding for broadcast communication, compared to a more robust full flooding algorithm.

To succeed in jamming, the jammer needs to both detect the sender, have a short enough response time, including the propagation delay, and also have a power advantage over the sender at the receiving node.

The results that are to be further discussed and analyzed below are based on the mean delivery ratio of packets in the communication network, shown in Figure 3.4 - Figure 3.9. The delivery ratio is calculated by measuring the total amount of packets transmitted and received in the entire network. Since broadcast traffic will be delivered to all other nodes, the delivery ratio is calculated as $\frac{p_{rx}/p_{tx}}{N-1}$ where p_{rx} is the total number of received packets, p_{tx} is the total number of transmitted packets and N is the number of nodes in the network. There is one figure each for the different combinations of flat, hilly or no terrain and using the OLSR (MPR-flooding) protocol or the full flooding algorithm. The parameters for the different plots in each figure are then jammer output power, whether the jammer is jamming control slots only or all slots (in case of OLSR routing), and the jammer response time.

3.5.1 Meeting the time criteria

First we analyse if the hop rate of the communication nodes can ”outrun” the jammer. In our case, we also have an erasure correction capability, according to Table 3.1 one third of a packet can be lost before the packet is dropped. From this, simplifying the argument in Equation 2.7 from section 2.1.4, we realize that the jammer can never successfully jam anything where $(T_r + T_{JR}) > \frac{2}{3}T_{dw}$, where T_r is the jammer response time, T_{JR} is the propagation delay between the jammer and the receiving node and T_{dw} is the frequency hop length, since the jammer needs to jam more than one third of the packet length. Using this with Table 3.2, a jammer response time of 100 μs can never successfully jam anything with hop rate 6 khop/s from a distance of 5 kilometer. A jammer response time of 25 μs on the other hand is harder to outrun. At a hop rate of 10 khop/s, the jammer can still theoretically jam more than one third of the slots from

a 5 kilometer distance. Although at larger distances, i.e. further into the network, the jammer will not be able to jam anything at 10 khop/s.

The results from simulations clearly shows this too, by looking at what hop rate the communication network manage to stay connected at. In Figure 3.4 - Figure 3.9 we can see that at a hop rate of 6 khop/s the communication network is no longer jammed when the jammer has a response time of 100 μs. In the case that the jammer response time is 25 μs, the networks with 10 khop/s only slightly affected by the jammer.

3.5.2 Terrain and power

As mentioned, the position of the jammer is critical here. A good position can give the jammer a line of sight to the target even for long distances, but a bad position can block the signal path entirely, especially in hilly terrains.

The resulting packet delivery ratio in the two terrains can be compared in Figure 3.4 - Figure 3.7. Although it is hard to draw a general conclusion from this because of the large variations due to the position of the jammer, our simulations show that the network in the flat terrain is more jammed than the network in the hilly terrain, even though the network in the flat terrain has better connectivity before it is jammed. The connectivity can be seen when looking at the results from full flooding without a jammer. The network is 100% connected in the flat terrain, Figure 3.7, but only 97% connected in the hilly terrain, Figure 3.5.

Looking back at Figure 3.2, note that the jammer position in the flat terrain is very favourable for the jammer. There, all the nodes in the communication network are located below the jammer. From the terrain profile for the hilly terrain, we see that there are more obstacles in the path between the jammer and the target nodes. It can also be noted, although not depicted here, that these obstacles are even bigger in some of the paths from the jammer to other spots in the communication network area, i.e. the path to the corners of the network area, while the flat terrain profile is relatively similar in all angles.

To get a better view of the network connectivity, Figure 3.3 shows snapshots of the network for the different terrain types. Here, all symmetrical communication links are marked blue and all jammed links are marked red. More specifically, the links considered jammed in this figure are symmetrical links that existed when there was no jammer. With the jammer present, only the blue symmetrical links are left. Firstly, note the different connectivity in the three different terrain types by observing the total number of communication link (jammed plus non-jammed). Secondly, notice that the jammed links are not necessarily only the ones that are closest to the jammer, especially in the case with the hilly terrain. Again, the terrain and the fact that the jammer needs to both detect the sender and have a power advantage on the receiver makes both short nearby links and distant long links harder to jam.

The results from the simulations with terrain can also be compared to simulations run with a simple plane earth model, where the path gain is calculated as in Equation 2.2 in section 2.1.1. The results shown in Figure 3.8 and Figure 3.9 differ a lot from the other results which shows the importance of using terrain in simulations of scenarios like this. Looking at the simulation results from the plane earth simulations, we see

that the jammer with 50 W output power is not able to do much damage. The jammer with 1000 W output power on the other hand totally kills the entire network for low frequency hop rates. In the plane earth simulation the network is fully connected and has a lot more links, i.e. alternative routes, than for the scenarios with terrain. 50 W jammer output power is simply not enough to knock them all out. When the jammer output is raised to 1000 W, the power overtake for the jammer is enough to take out almost the entire network. These results show that the terrain will both cause lower connectivity in the network, but also creates a certain protection from a single jammer. This is most clearly seen in the results of the scenario with the 1000 W jammer. We know from the plane earth reference simulation that the jammer has a power advantage, but it still does not succeed in jamming the flat terrain quite as well, and in the hilly terrain it has an even harder time to jam the network.

3.5.3 Routing protocol

To investigate the effect of jamming the network routing protocol, different simulations are run using either OLSR or full flooding. In our simulations, all traffic is broadcast traffic, which means that OLSR imply MPR-flooding.

In our simulations, the network is quite sparse. As mentioned before, we can see that the network is fully connected in the flat terrain but only 97% connected in the hilly terrain. While using OLSR the delivery ratio of the non-jammed, fully connected network in the flat terrain is 98% and only 94% in the hilly terrain. In the results from the simulations with OLSR, in Figure 3.4, Figure 3.6 and Figure 3.8, we can see the effect of loosing the MPRs when they are jammed. When jamming all slots, OLSR is more vulnerable than the more robust full flooding algorithm.

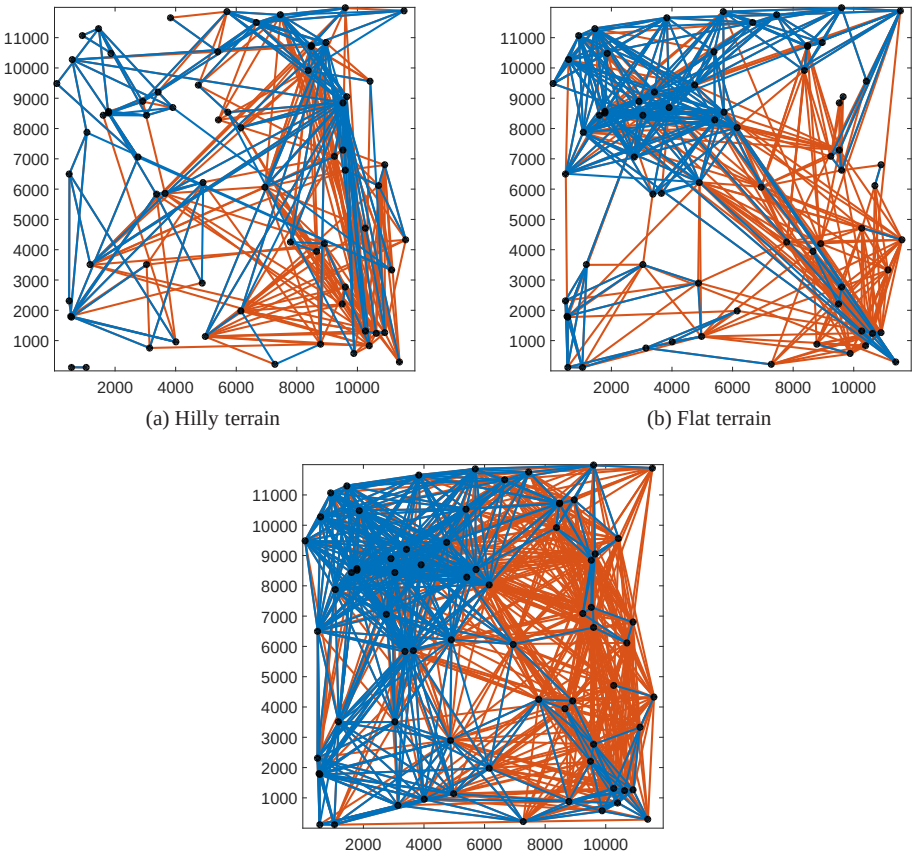
As another experiment on the robustness of OLSR, we let the jammer be more intelligent by only jamming the control slots where the Hello messages are sent. The results are shown as the dashed lines in Figure 3.4, Figure 3.6 and Figure 3.8. The simulation results show that this is enough to have an impact on the network delivery ratio. What happens when the Hello messages are jammed is that the links are considered bad by the protocol and are not used as MPRs to relay data on. Although the closest neighbours (one hop neighbours) will still be able to receive packets over these links.

3.5.4 Simulation result conclusions

From our simulations we can see that the terrain has great influence on the network, both on the connectivity of the communication network alone and in a scenario with a follower jammer. The positioning of such a jammer is critical when measuring the impact of the jamming. Although it is hard to draw a general conclusion from this because of the large variations due to the position of the jammer, our simulations show that the network in the flat terrain is more jammed than the network in the hilly terrain, even though the network in the flat terrain has better connectivity before it is jammed. Hence, the terrain will both cause lower connectivity in the network, but also create a certain protection from a jammer. Together with the fact that the jammer needs to both

detect the sender and have a power advantage on the receiver, the hilly terrain makes it harder to jam a communication link, since the probability is higher for any one of the two nodes to be located behind terrain obstacles.

When investigating the network protocol in a scenario with a follower jammer, we compare OLSR MPR-flooding with a full flooding algorithm. Note, full flooding provides the best delivery ratio that can be obtained given the jammed links in the network. The results show that although OLSR MPR-flooding is not as robust as full flooding, it is still relatively robust. In the case of an intelligent follower jammer, which only jams the OLSR control traffic, the impact on the network delivery ratio is evident, although not as high as when jamming all traffic.



(a) Hilly terrain

(b) Flat terrain

(c) Plane earth model (no terrain)

Figure 3.3: A snapshot of the network links. The communication network is running the OLSR protocol has a frequency hop rate of 4 khop/s. The jammer has an output power of 50 W and a response time of 100 μs and is located 5 km to the right of the network plot. Jammed links are marked red and non-jammed communication links are marked blue.

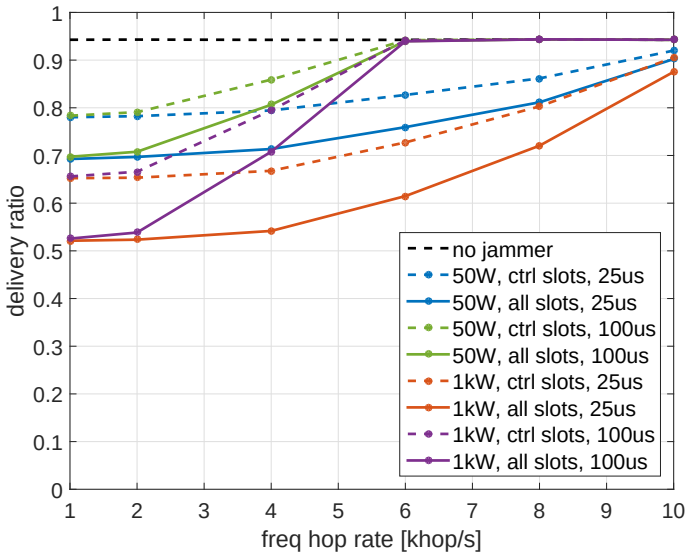


Figure 3.4: Delivery ratio in network running **OLSR** protocol for broadcast communication (MPR-flooding) in **hilly terrain**. The parameters for the different plots are jammer output power, whether the jammer is jamming control slots only or all slots, and the jammer response time.

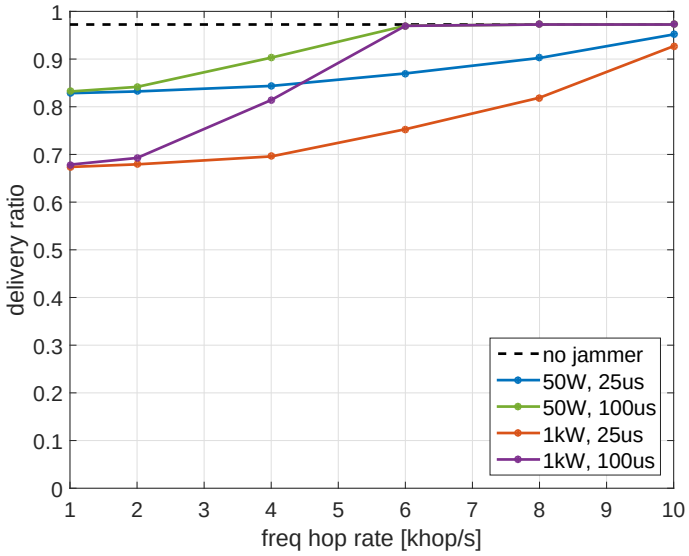


Figure 3.5: Delivery ratio in network with **full flooding** broadcast communication in **hilly terrain**. The parameters for the different plots are jammer output power and the jammer response time.

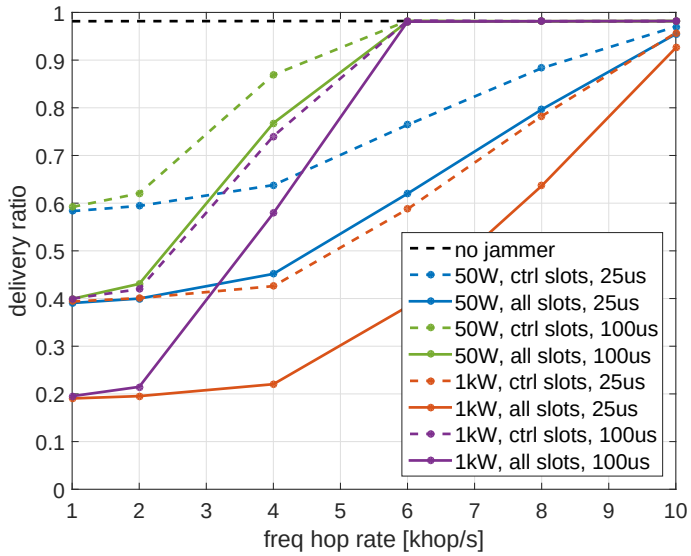


Figure 3.6: Delivery ratio in network running **OLSR** protocol for broadcast communication (MPR-flooding) in **flat terrain**. The parameters for the different plots are jammer output power, whether the jammer is jamming control slots only or all slots, and the jammer response time.

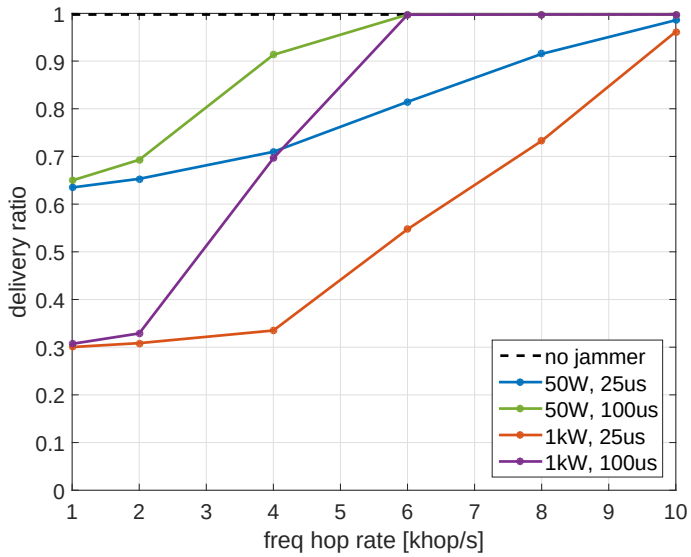


Figure 3.7: Delivery ratio in network with **full flooding** broadcast communication in **flat terrain**. The parameters for the different plots are jammer output power and the jammer response time.

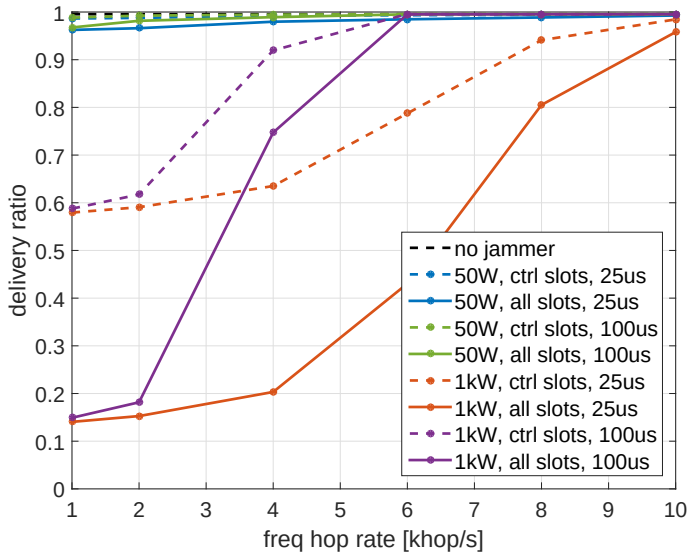


Figure 3.8: Delivery ratio in network running **OLSR** protocol for broadcast communication (MPR-flooding) in a plane earth simulation model, i.e. **no terrain**. The parameters for the different plots are jammer output power, whether the jammer is jamming control slots only or all slots, and the jammer response time.

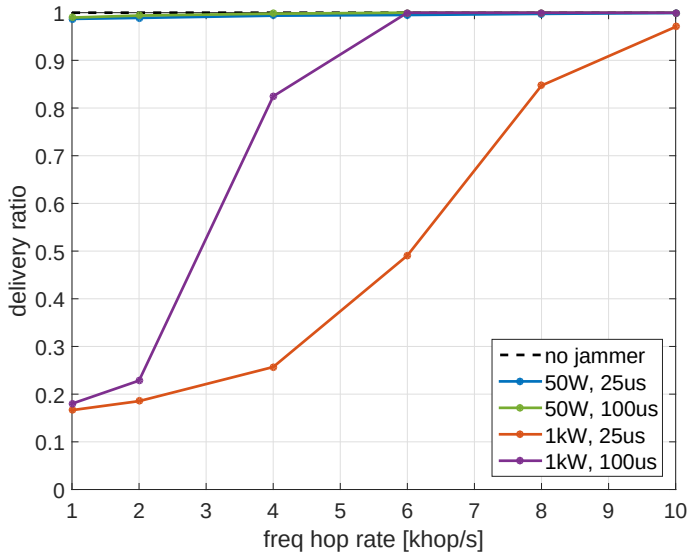


Figure 3.9: Delivery ratio in network with **full flooding** broadcast communication in a plane earth simulation model, i.e. **no terrain**. The parameters for the different plots are jammer output power and the jammer response time.

4 Conclusions

How to provide protection against jamming is an important issue for tactical radio network performance. Frequency hopping (FH) is an often used jamming protection technique. However, an adaptive jammer, as a fast follower jammer, can be a serious threat to a tactical ad hoc network using FH. The threat can be regarded as increasing, as very capable real time spectrum analyzers and waveform generators are commercially available and fast follower jammers can be built based on such commercial equipment. Another, non-adaptive, FH jamming threat is partial-band noise jamming.

In this report, ad hoc networks exposed to jamming are examined. An approximative analytical method based on three separate follower jammer criteria is devised (detection, power and time). We compare the three criterias for follower jamming with the power criteria for the partial-band jammer. Sixteen jammer-communication system combinations has been evaluated, based on all combinations of four system options: (1) a weak or a strong jammer (power and antenna gain), (2) a slow or a fast jammer (response time), (3) a low or a high frequency hop rate, (4) a narrow band (NBWF) or a wideband waveform (WBWF).

We summarize what is the best option for the jammer in those sixteen jammer-communication examples. A large available bandwidth makes partial-band jamming difficult. The partial-band jammer is rather competitive, when compared to the follower jammer for WBWF with a rather small number of channels to hop on, but inferior the follower jammer for NBWF with a large number of channels to hop on. Follower jamming is preferable for the fast follower jammer option against NBWF. The time criteria is critical for the slow follower jammer performance against NBWF with low hop rate. Here the erasure correction capability decides whether follower jamming or partial-band jamming is preferable. For the high hop rate, the time criteria makes follower jamming useless and the partial-band jammer must be used. For jamming with the weak jammer against WBWF, we note that partial-band jamming is preferable because the difference in the power criteria is quite small between the partial-band jammer and the follower jammer. For jamming with the strong jammer against WBWF, there is a larger difference in the power criteria between the partial-band jammer and the follower jammer. Follower jamming is preferable for the slow hop rate in this case. For the high hop rate, the time criteria makes the follower jamming range small compared to partial-band jamming and therefore partial-band jamming is preferable.

In order to study the network properties under follower jamming, event based network simulations are performed. Focus is to examine how the terrain and the network protocols influence the jamming resistance. To measure the performance of the network the packet delivery ratio is used. The terrain influences how easy it is to jam a network. Two areas with different terrain types are tested. An area in northern Sweden with hilly terrain and an area in the south of Sweden where the terrain is more flat. As a reference, a plane earth model is also tested as the flat terrain still has some hills and vegetation and is far from a plane earth model. The network in the flat terrain becomes more jammed than the corresponding network in the hilly terrain. The fact that the jammer needs to both detect the sender and have a power advantage on the receiver makes it harder to jam in a hilly terrain than in a flat terrain. Of interest

in the jamming robustness of the network protocols, we investigate a network using OLSR MPR-flooding and compare with a network using full flooding. Also, we study the effects of intelligent jamming that take advantage of the routing protocol structure and only jam the protocol control traffic. Even if not as robust as full flooding, OLSR MPR-flooding is still fairly robust under jamming. To only jam the control protocol traffic has an impact on the network delivery ratio, but not as high impact as when all traffic is jammed.

References

[1] A. Hansson, J. Nilsson, and K. Wiklundh. Performance analysis of follower jamming of frequency-hopping ad hoc networks with random dwell-time. In *MILITARY COMMUNICATIONS CONFERENCE, MILCOM*, Tampa, USA, 2015.

[2] A. Hansson, J. Nilsson, and K. Wiklundh. Follower jamming of ad hoc networks. Report FOA-R–4060–SE, Swedish Defence Research Agency., Linköping, Sweden, February 2015. In Swedish.

[3] M.K. Simon, J.K Omura, R.A. Scholtz, and B.K. Levitt. *Spread Spectrum Communications*. Computer Science Press, 1985.

[4] D.J. Torrieri. Fundamental limitations on repeater jamming of frequency-hopping communications. *IEEE Journal on selected areas in communications*, 7(4), October 1989.

[5] Rohde & Schwarz. ESU EMI Test Receiver, Version 02.00, October 2007. `https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/ESU_dat_sw_en_v02.pdf`.

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

[7] P. Holm. Detvag-90. Use of the Ground-Wave Program GRWAVE in theWave-Propagation Model DETVAG. Technical Report C 30678-3.5, Defence Research Est., Div. of Command and Control Warfare Tech. Linköping, Sweden, feb 1993. In Swedish.

[8] T. Clausen and P. Jacquet (Editors). Optimized link state routing protocol (OLSR). In *IETF, Request for Comments 3626*, Oct 2003.

[9] J. Macker. Simplified multicast forwarding (SMF). Internet-draft, IETF, Network Working Group, January 2012.

[10] J. Nilsson and U. Sterner. Robust MPR-based flooding in mobile ad-hoc networks. In *MILITARY COMMUNICATIONS CONFERENCE, MILCOM*, Orlando, USA, 2012.

FOI, Swedish Defence Research Agency, is a mainly assignment-funded agency under the Ministry of Defence. The core activities are research, method and technology development, as well as studies conducted in the interests of Swedish defence and the safety and security of society. The organisation employs approximately 1000 personnel of whom about 800 are scientists. This makes FOI Sweden's largest research institute. FOI gives its customers access to leading-edge expertise in a large number of fields such as security policy studies, defence and security related analyses, the assessment of various types of threat, systems for control and management of crises, protection against and management of hazardous substances, IT security and the potential offered by new sensors.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se