

# Styrkor och svagheter hos militära respektive civila digitala radiosystem

Prof. Peter Stenumgaard  
Forskningschef

# Innehåll

- Bakgrund till skillnader mil/civ system
- Störtålighet kontra kapacitet
- Systemexempel
- Slutsatser

# Wireless Systems are widely used in lots of applications



# Trådlös teknik

## Fördelar

- Hög flexibilitet; kräver inga kablar

## Nackdelar

- Känslig för oavsiktliga störningssignaler i luften
- Känslig för avsiktlig störning

# Nya datorer slår ut gps

## Högfrekventa processorer kan skapa störningar för SOS Alarm

Nya datorer stör ut gps-mottagare. En bärbar dator i en ambulans kan innebära katastrof.

- Det skulle vara mycket, mycket besvärande om vi inte får rätt information om ambulansernas situation, säger Anders Klarström på SOS Alarm.

- Operatörerna dirigerar ambulanser bland annat utifrån gps-information. Beroende på om de står still i köer, var de är och vart de ska så fattas besluten, säger Anders Klarström.



Anders Klarström.

En ny undersökning från Försvarets forskningsinstitut, FOI, visar nu att helt vanliga datorer kan störa ut gps-mottagare. Det är datorernas allt snabbare processorer som skapar störningar i det frekvensband där gps-signalen ligger. När samma undersökning gjordes för fem år sedan fanns inte problemen.

- Nu börjar situationen bli allvarig. För pratade man om att atombomber kunde slå ut olika system i ett jas-plan. Nu slår vanlig elektronik ut viktiga system. Ofta vet man inte varför en gps-mottagare visar fel eller blir svart, säger Peter Stenumgaard på FOI.

Tidigare har oron kring gps-hund-sakligen rört systemets sårbarhet vid aktiv störning i samband med brutt. De nya bevisen för att vanlig vardagsteknik slår ut mottagarna sätter frågan i ett annat sammanhang. Delvis därför att gps används allt mer i viktiga samhällssystem, som automatisk positionering vid olyckor och andra



Peter Stenumgaard.

larmtjänster. Cirka 600 av landets ambulanser styrs delvis utifrån gps-information.

- Vi har redan gått ut och varnat militära styrkor för följderna av störningarna. Naturligtvis kan det orsaka stor skada även civilt, säger Peter Stenumgaard.

Och på SOS Alarm ser man allvarigt på situationen. Förutom ambulanserna är många personlarm utrustade med en gps-funktion för lägesbestämning. Bara SOS Alarm har drygt 7 000 larm ute. Exempelvis används dessa av Vattenfalls linjereparatörer och ensamstående kronofogdar.

- När det gäller personlarm har det förekommit att positionen inte har uppdaterats på ett antal timmar, säger Anders Klarström.

Olle Nygårds 08-796 65 09  
olle.nygards@nyteknik.se

### Civil gps känsligare än militärens

● Gps-signalen sänds på frekvenserna 1,6 GHz för civilt bruk och 1,2 GHz för militärt bruk.

● Militär signal har bandbredd 20 MHz, civila har 2 MHz. Det gör den civila mer känslig.

## Ny dator förstör din GPS

Nya datorer kan slå ut GPS-mottagare, visar en undersökning från Försvarets forskningsinstitut, FOI. SOS Alarm riskerar därmed stora störningar i ambulans- och larmverksamheten.

Det är de nya datorernas allt snabbare processorer som skapar störningar i det frekvensband som GPS-signalerna ligger på.

- Vi har redan gått ut och varnat militära styrkor för följderna av störningarna, säger Peter Stenumgaard på FOI till Ny Teknik.

(Aftonbladet)



En bärbar dator i en ambulans kan betyda att SOS Alarm inte får information om ambulansens läge.

Intersystem-interference triggered the self-destruction mechanism in the UAV *Global Hawk* during test flight\*)



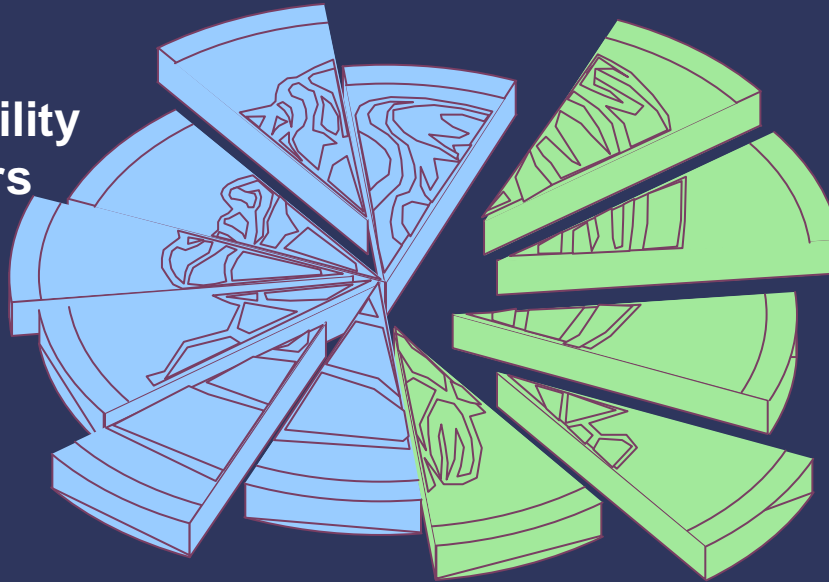
\*) Institute for Defense Analyses (IDA)

# Civilian vs military telecommunications

Driving forces behind technical properties

## Commercial interests:

- Capacity
- Coverage & availability where the customers are
- Low price
- Low power
- Existing infrastructure



## Military special requirements:

- Robustness against interference
- Stealth properties
- Peer-to-peer
- High requirements for real-time applications
- Network planning on the move.
- Create infrastructure during mission

# Robustness vs Capacity – you can never get both

Robustness against  
interference

Capacity



- Requires redundancy
- "Steals capacity"
- Military applications
- Desirable in critical safety & security applications
- Desirable in critical industrial applications

- As less redundancy as possible e.g. high data rate.
- "Steals robustness"
- Civilian consumer electronics"

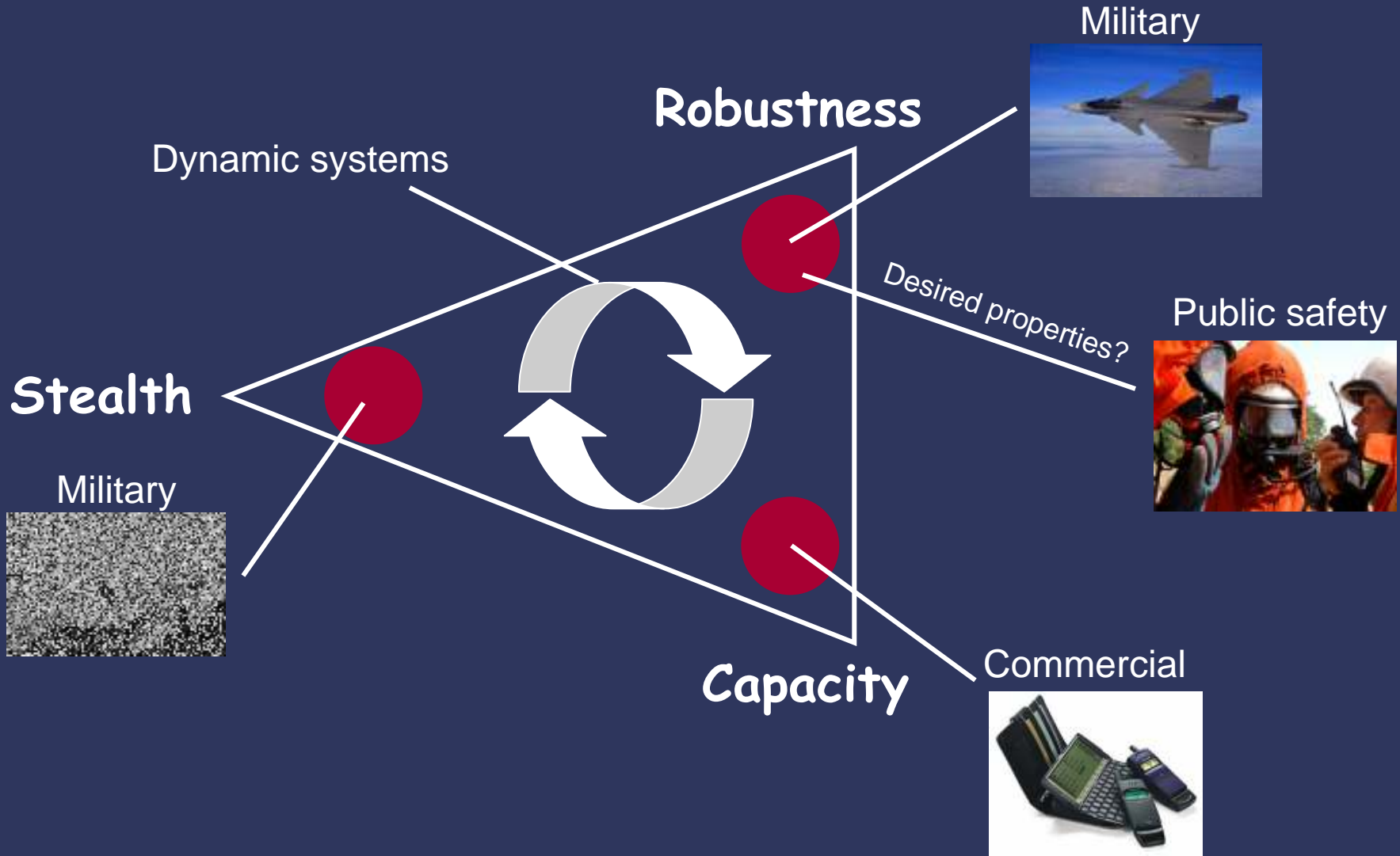
# Störtålighet

- ❖ Störtålighet innebär att en del av dataströmmen används till redundant information. Redundansen ökar systemets tålighet (eng. robustness) mot störningar
- ❖ Exempel på redundans kan vara
  - Större frekvensband än nödvändigt
  - Redundanta (extra) datasymboler i dataströmmen
- ❖ Ökad störtålighet stjäl alltså resurser som t ex skulle kunna användas till högre dataakt/kapacitet

# Do not mix up encryption with robustness against interference!

- ❖ Encryption means that an illegal actor can not get out any information from the communications.
- ❖ Robustness means that an illegal actor can not disturb the communications by the use of interference signals.

# Stealth – another dimension for military systems

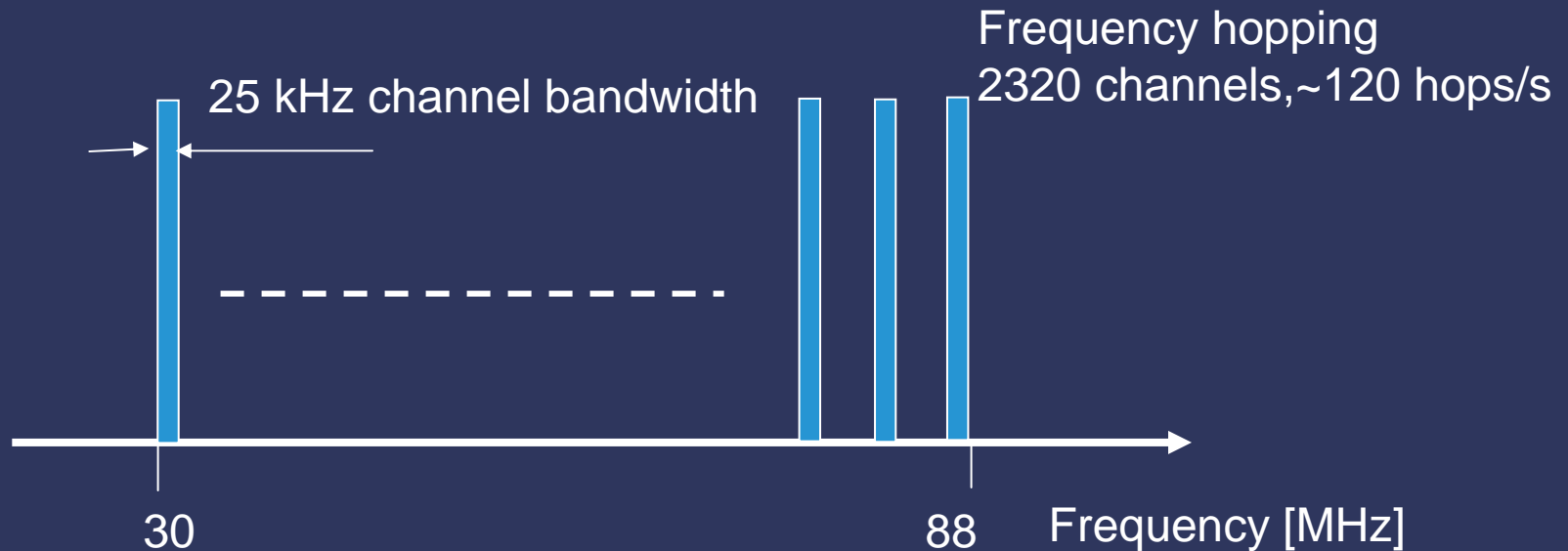




IEEE EMC Karlskrona 2008-09-04

# Example: Army combat radio Ra 180/480

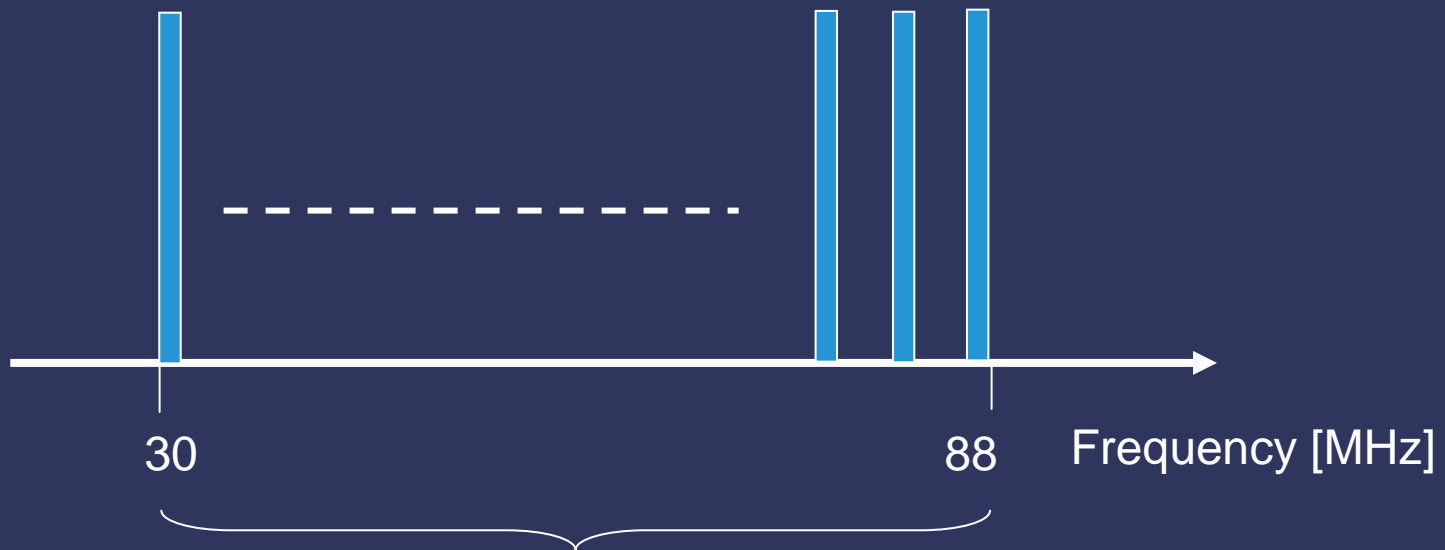
## Optimized for robustness against interference



- Processing gain  $10\log(58/0.025) = 34$  dB
- The radio uses 2320 times more bandwidth than necessary for its data rate.
- This extra redundancy is used as increased robustness against interference.

# Example: Army combat radio Ra 180/480

A jammer must use 2320 times higher power to create the same damage compared to if the radio only used one channel

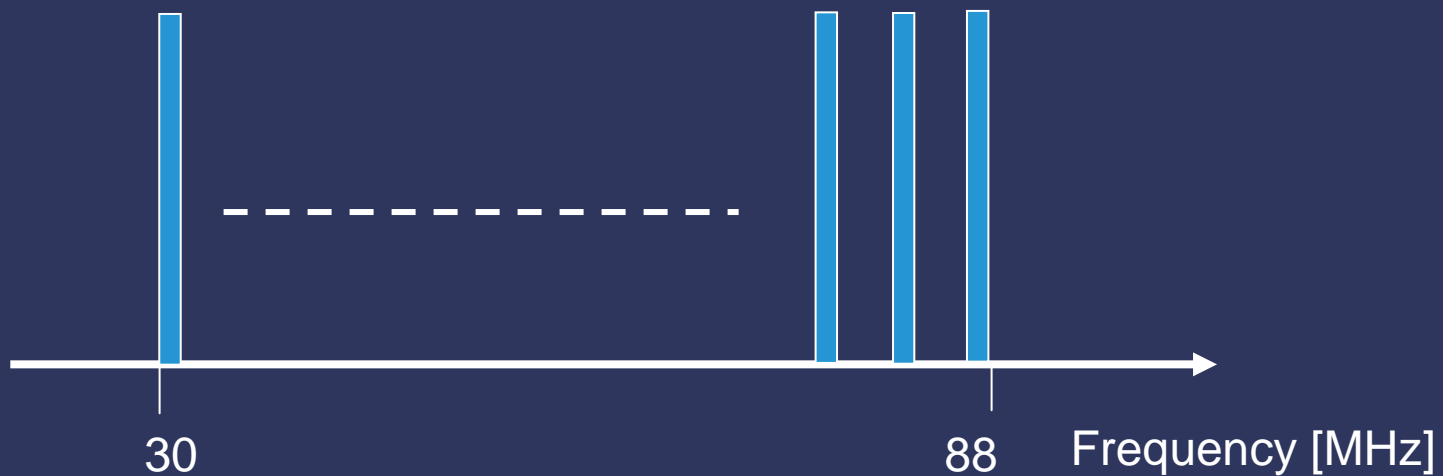


The jammer must spread its power over a larger bandwidth

# Example: Army combat radio Ra 180/480

Number of channels disturbed	Resulting bit error probability (BEP)
1	$2 \cdot 10^{-4}$
2320	0.5

The robustness reduces the BEP from 0.5 to  $2 \cdot 10^{-4}$



# Example:TETRA

- TETRA specifications were optimized for public safety requirements in Europe.
- Mobile base stations (~50 km), peer-to-peer (~3 km) communication

## Frequency bands

380-390 UL / 390-400 DL

410-420 UL / 420-430 DL

450-460 UL / 460-470 DL

## Physical layer

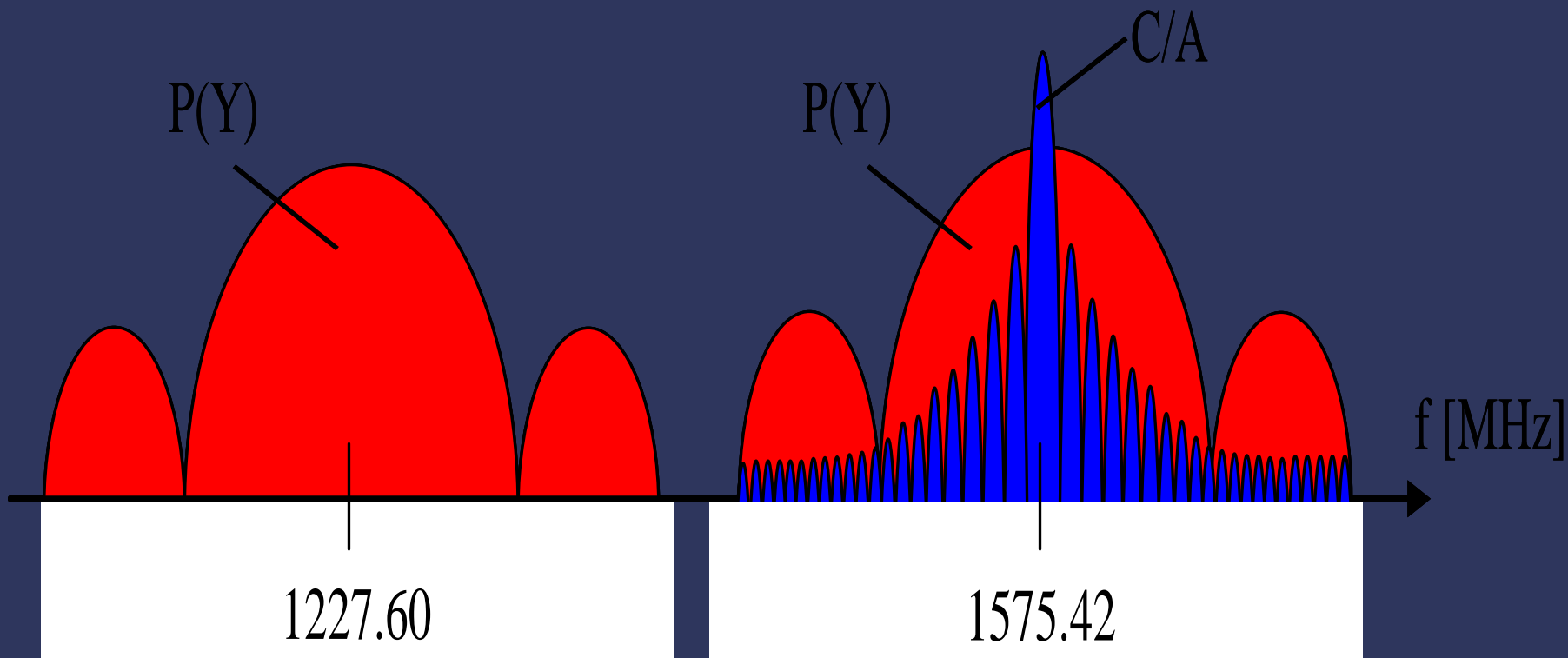
- Channel bandwidth 25 kHz, TDMA 4 time slots
- Modulation  $\pi/4$  DQPSK
- Bitrate 7.2 kbit/s for speech
- Error-correcting codes for increased range, not for increased robustness

# Example: TETRA

❖ No certain robustness against interference

- No extra redundancy for robustness
- Small frequency region => no large improvements if frequency hopping had been used.
- Easy to jam, vulnerable for unintentional interference
- Encrypted traffic => difficult for an illegal actor to extract information from the signal

# Military vs civilian GPS systems



— Military, 20 MHz bandwidth  
— Civilian, 2 MHz bandwidth

# The vulnerability is explored by illegal actors

## Riots during the EU summit in Gothenburg 2001

Demonstrants take advantage of the sensitivity of the police's radio system to interference and manage to prevent communication during critical phases of the riots.

## Car burglary

Criminals have used jammers to block the remote control receiver for car keys to prevent the owner to lock the car. When the owner leaves the car it is emptied by the criminals.

## A market for illegal jammers

Products, schematics and components for jamming is today easy to buy on the internet.

# Wireless in safety & security

- ❖ It is hazardous to use standard civilian wireless products in applications that need large robustness against interference.
- ❖ For industrial applications, the interest of robustness against interference is growing due to higher needs of reliable wireless systems.