Jamming Jammers
Jamming GSM Phones

ROYAL INSTITUTE
OF TECHNOLOGY

Daniel Månsson
Division for Electromagnetic Engineering
School of Electrical Enginnering
Royal Institute of Technology, KTH

manssond@kth.se

Summary:

- Jammers were investigated by the use of a reverberation chamber.

- Their interference ability were tested (successfully) against commercial GSM phones.

- The susceptibility of the jammers themselves was tested in a reverberation chamber.

KTH VETENSKAP OCH KONST

ROYAL INSTITUTE OF TECHNOLOGY

Reasons for the society’s increased vulnerability to IEMI.

Victim side	Source side
Increased use of sophisticated and sensitive **COTS** (Commercial-Off-The-Shelf) electronics.	More **commercial EM sources** that can act as weapons. Also, commercial sources used for a variety of EMC testing, which also can be used for IEMI.
Miniaturization of components and lower signal levels are used in systems.	**More components** available that can be assembled to homemade sources (e.g., switches, capacitors, magnetrons etc.). Much information via Internet.
More open ports that can be disturbed (e.g., antennas for wireless systems and power-, data- and lamp sockets for injection of disturbances).	IEMI attacks (rather than traditional terrorist acts) can be **performed anonymously** and covertly – long time to determine the cause of failure (compared to an explosion).
Physical **boundaries** of systems may not apply or coincide with electromagnetic zone boundaries.	

“Easy” to improve upon

Hard to improve upon

GSM jammer tested

ROYAL INSTITUTE OF TECHNOLOGY

Three samples of handheld GSM jammer:

o Low-cost (≈ 160 USD), cheaper if produced in large quantities directly from electronic components.

o Commercially available on the internet.

✓ Internet search gives the price ranges for other jammers from ≈ 20 - 2500 USD.

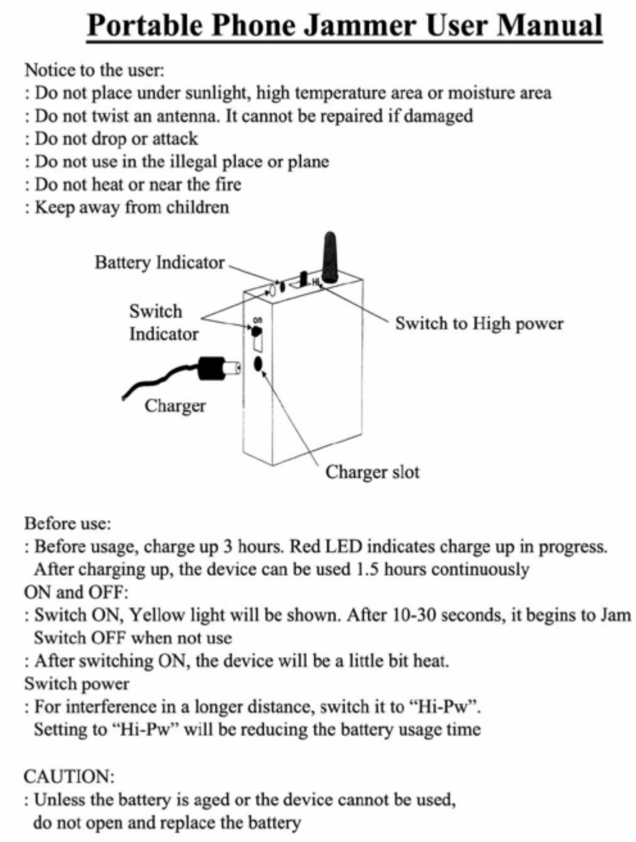
o “Userfriendly”.

o Isotropic frequency band specific noise emitter.

✓ Noise band emitted in 850 / 900 / 1800 / 1900 MHz.

✓ Not 3G, CDMA or TDMA.

✓ However newer version covers larger bands.



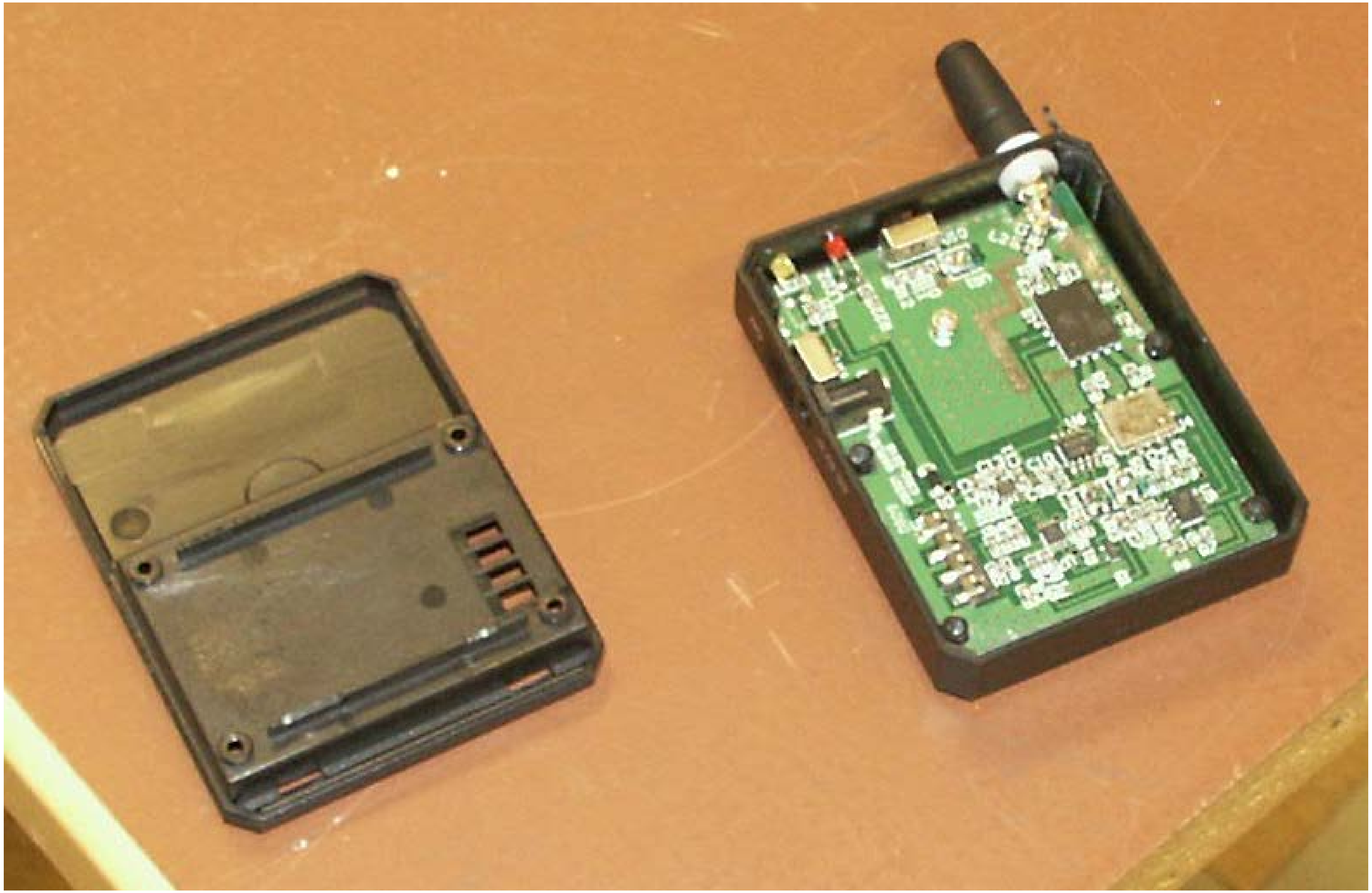
Portable Phone Jammer User Manual

Notice to the user:
: Do not place under sunlight, high temperature area or moisture area
: Do not twist an antenna. It cannot be repaired if damaged
: Do not drop or attack
: Do not use in the illegal place or plane
: Do not heat or near the fire
: Keep away from children

Battery Indicator
Switch Indicator
Switch to High power
Charger
Charger slot

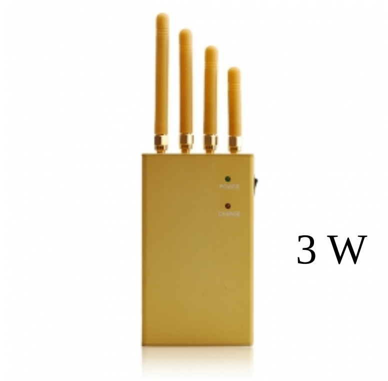
Before use:
: Before usage, charge up 3 hours. Red LED indicates charge up in progress.
After charging up, the device can be used 1.5 hours continuously
ON and OFF:
: Switch ON, Yellow light will be shown. After 10-30 seconds, it begins to Jam
Switch OFF when not use
: After switching ON, the device will be a little bit heat.
Switch power
: For interference in a longer distance, switch it to “Hi-Pw”.
Setting to “Hi-Pw” will be reducing the battery usage time

CAUTION:
: Unless the battery is aged or the device cannot be used,
do not open and replace the battery



Other commercial jammers of the Internet

120 W



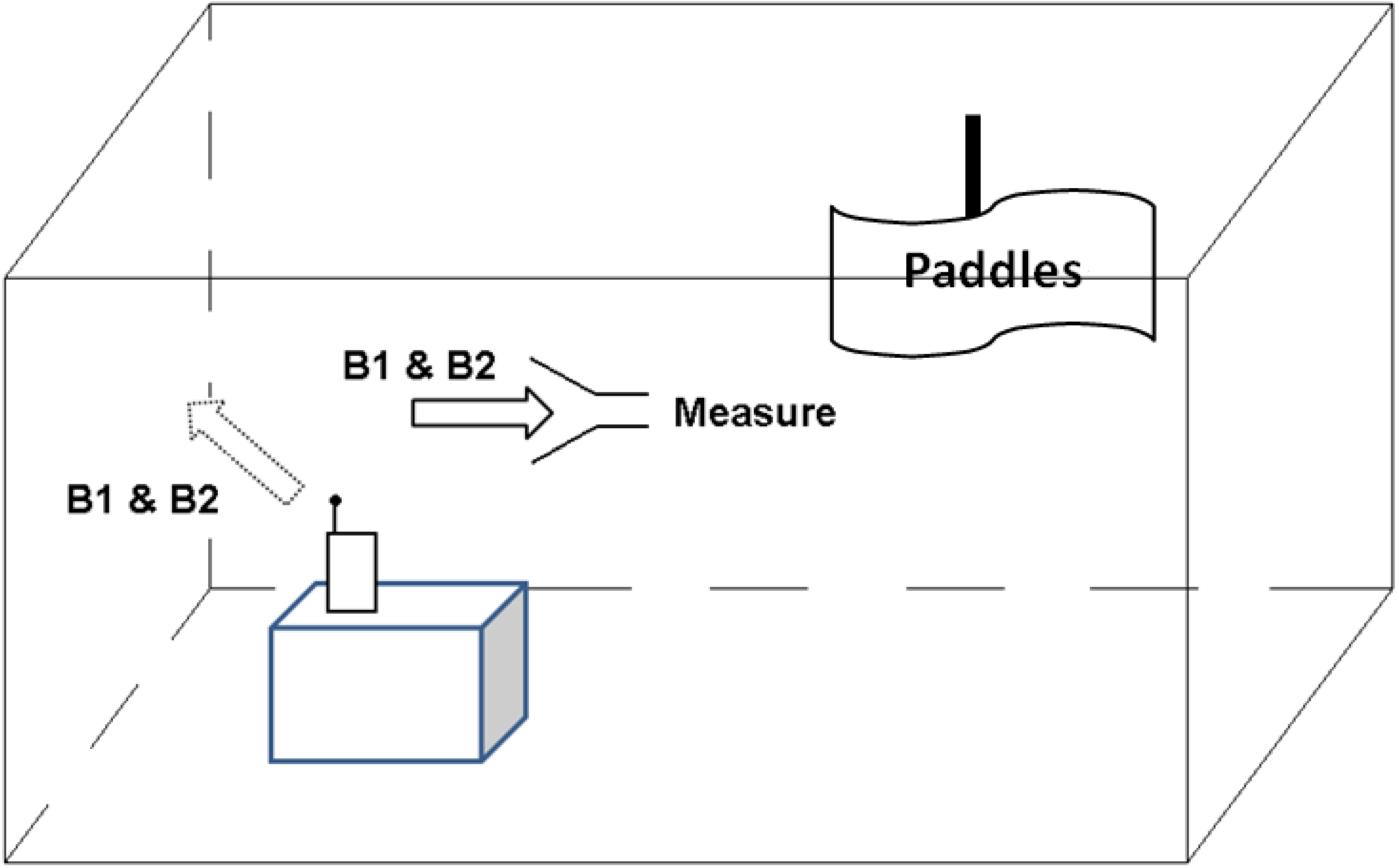
3 W

ROYAL INSTITUTE
OF TECHNOLOGY

1 W

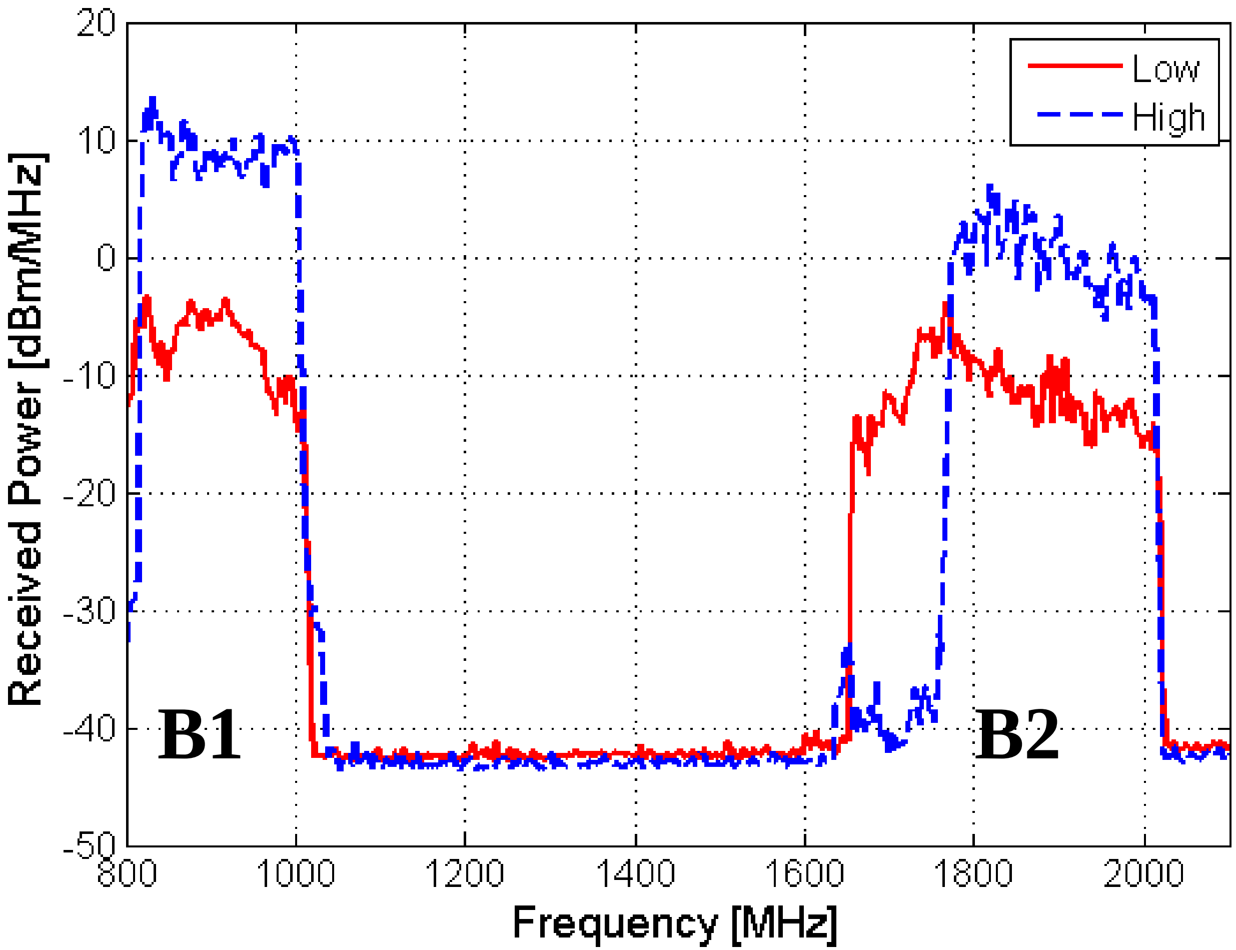
32 W

The output spectrum of the jammers

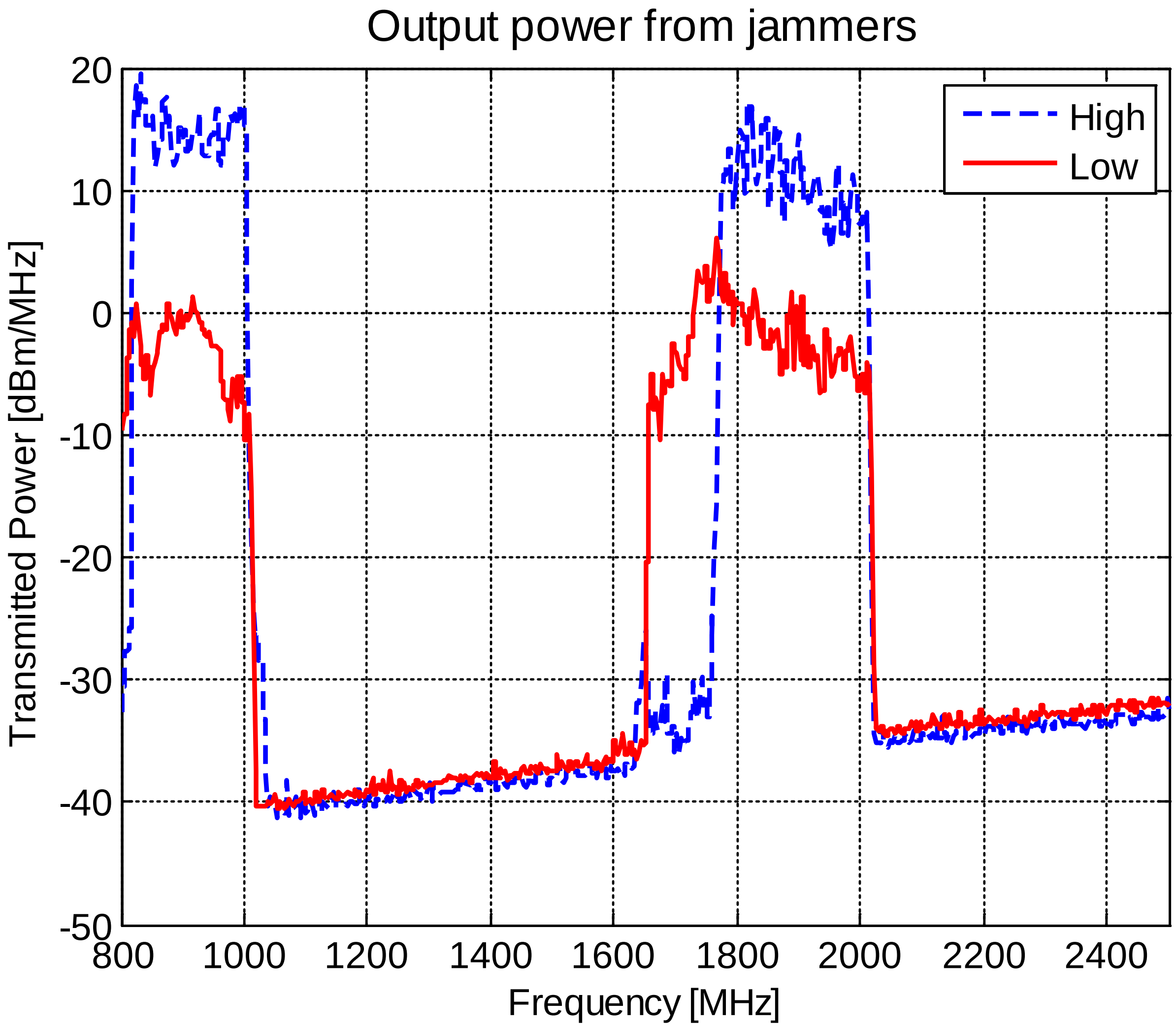


ROYAL INSTITUTE OF TECHNOLOGY

Received power spectra for the different states.



ROYAL INSTITUTE
OF TECHNOLOGY

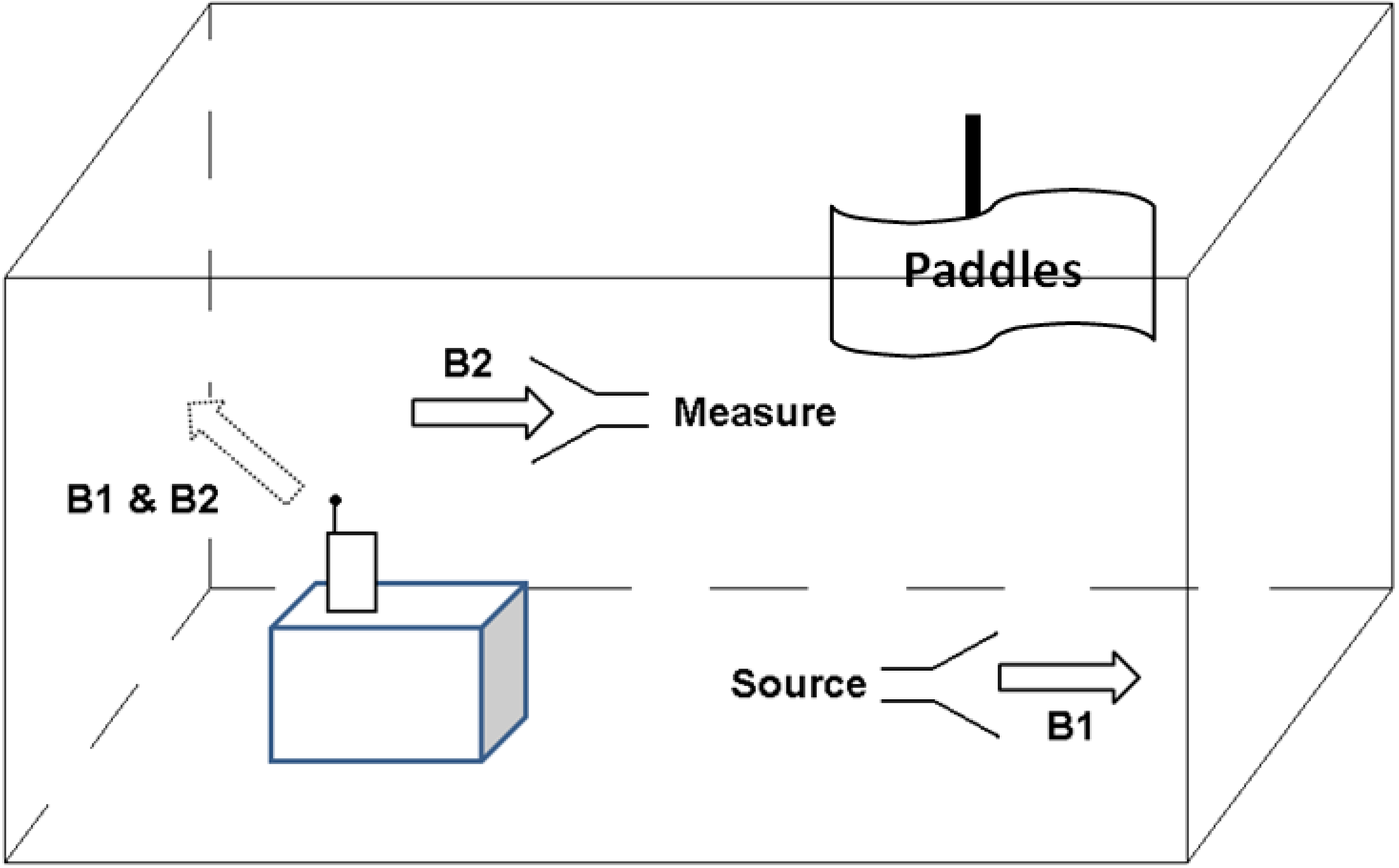


$$P_t = \langle P_r \rangle \frac{16\pi^2 V}{\lambda^3 Q}$$

Successful in jamming the operations of GSM phones according to the specification.

However, 3G enabled phone not affected.

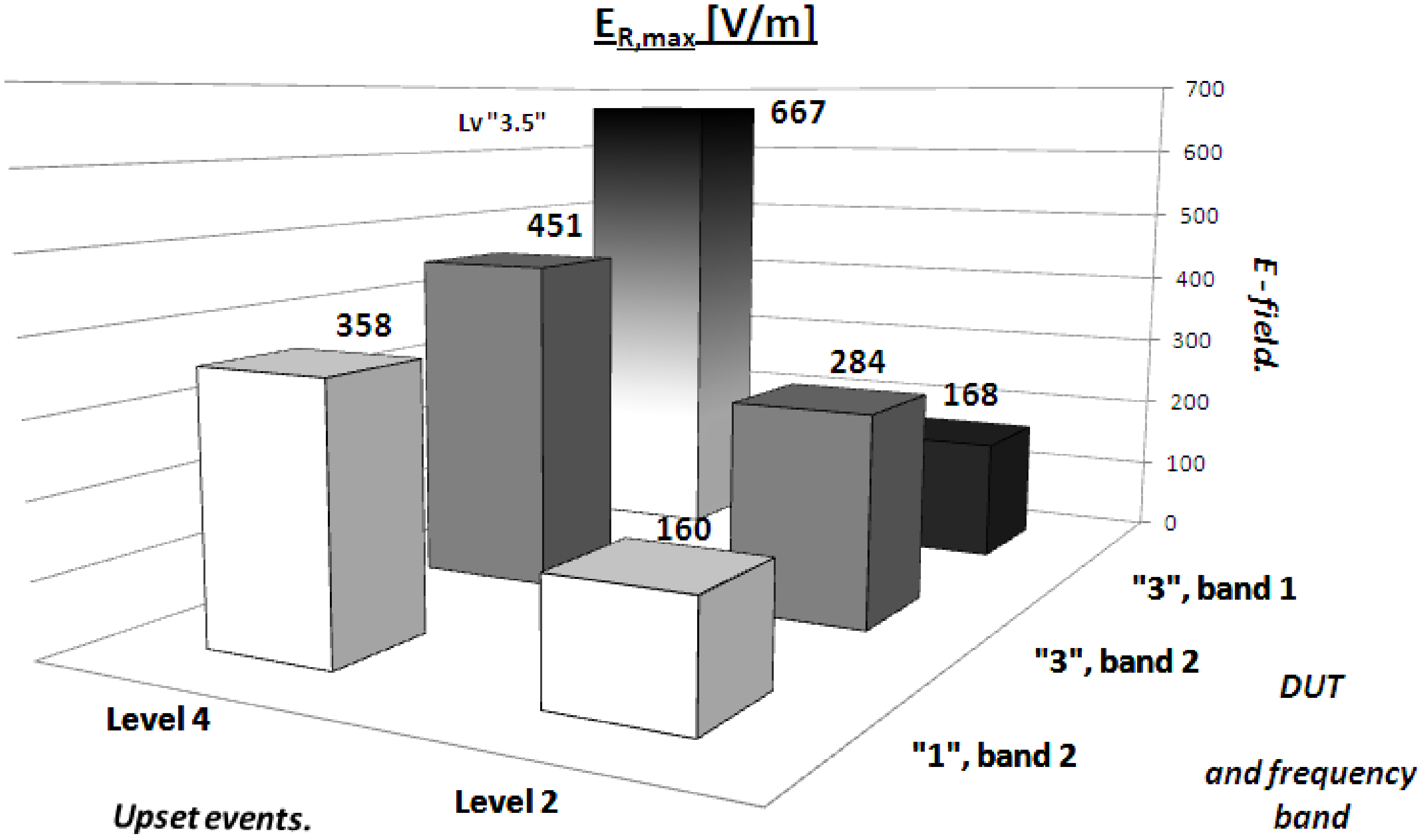
Susceptibility of the jammers



The disturbance used on the jammers is a CW signal.

KTH VETENSKAP OCH KONST

ROYAL INSTITUTE OF TECHNOLOGY



Level 1: No observed effect.

Level 2: Interference while exposed.

Level 3: Strong interference / crash, self- recovery.

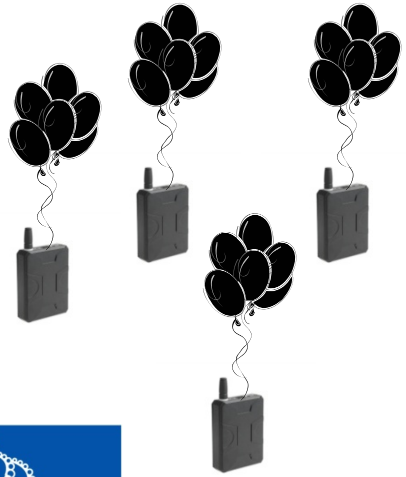
Level 4: Loss of function / crash, operator-intervention.

Level 5: Physical damage, repair or replace.

- “2” permanently damaged (Level 5) at ≈ 530 V/m.
- At 1.3 GHz: “1” Level 4 (Out-of-band) EMI.

This susceptibility data is used to investigate a countermeasure method against the jammers.

Balloon-jammers setup



An IEMI scenario using balloons to lift a large number of jammers over a, e.g., crowd in a city is assumed.

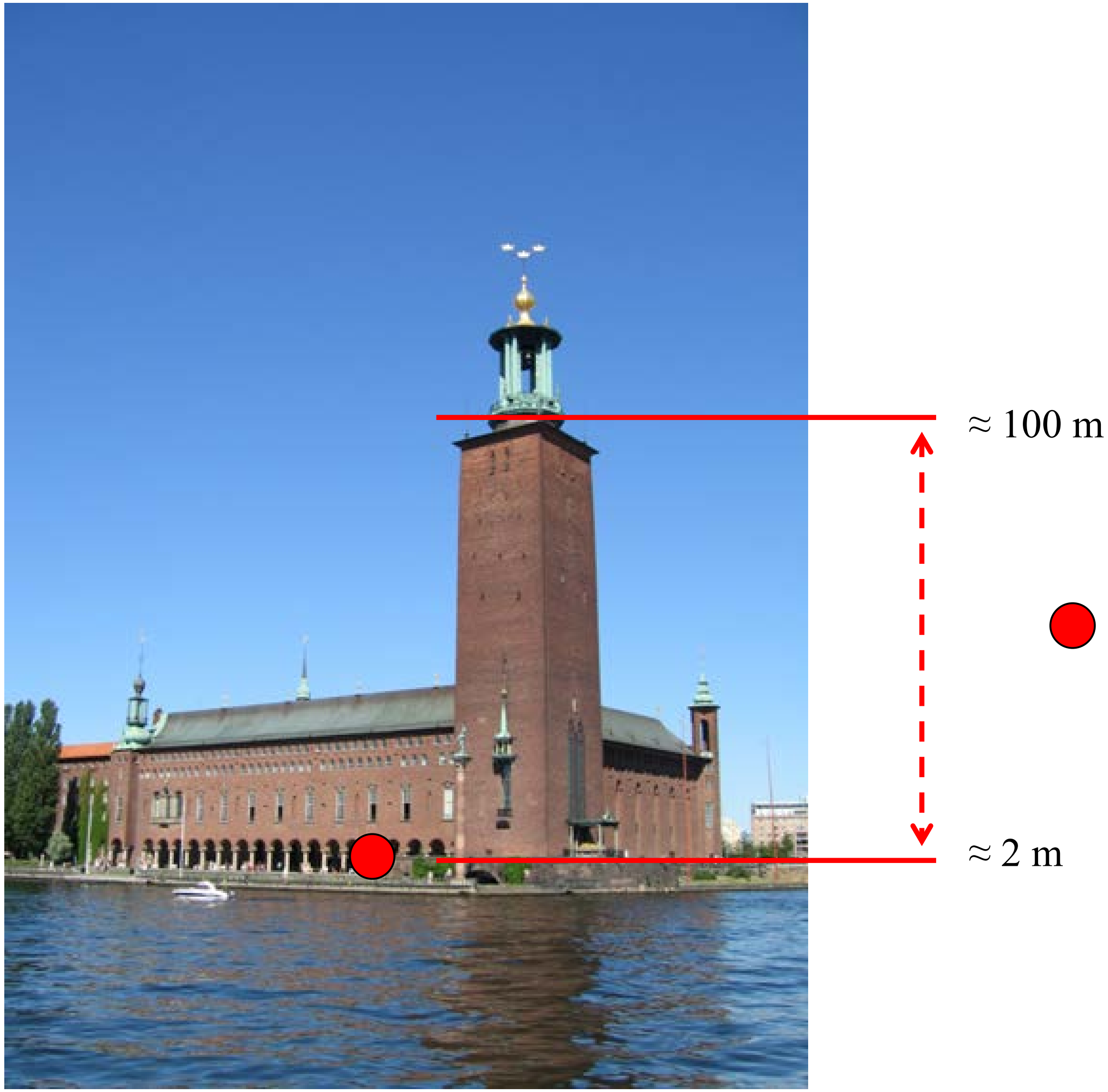
It could be difficult for law enforcement to easily counteract these interference sources.

However, a highly directive HPEM source could disrupt the jammers

KTH VETENSKAP OCH KONST

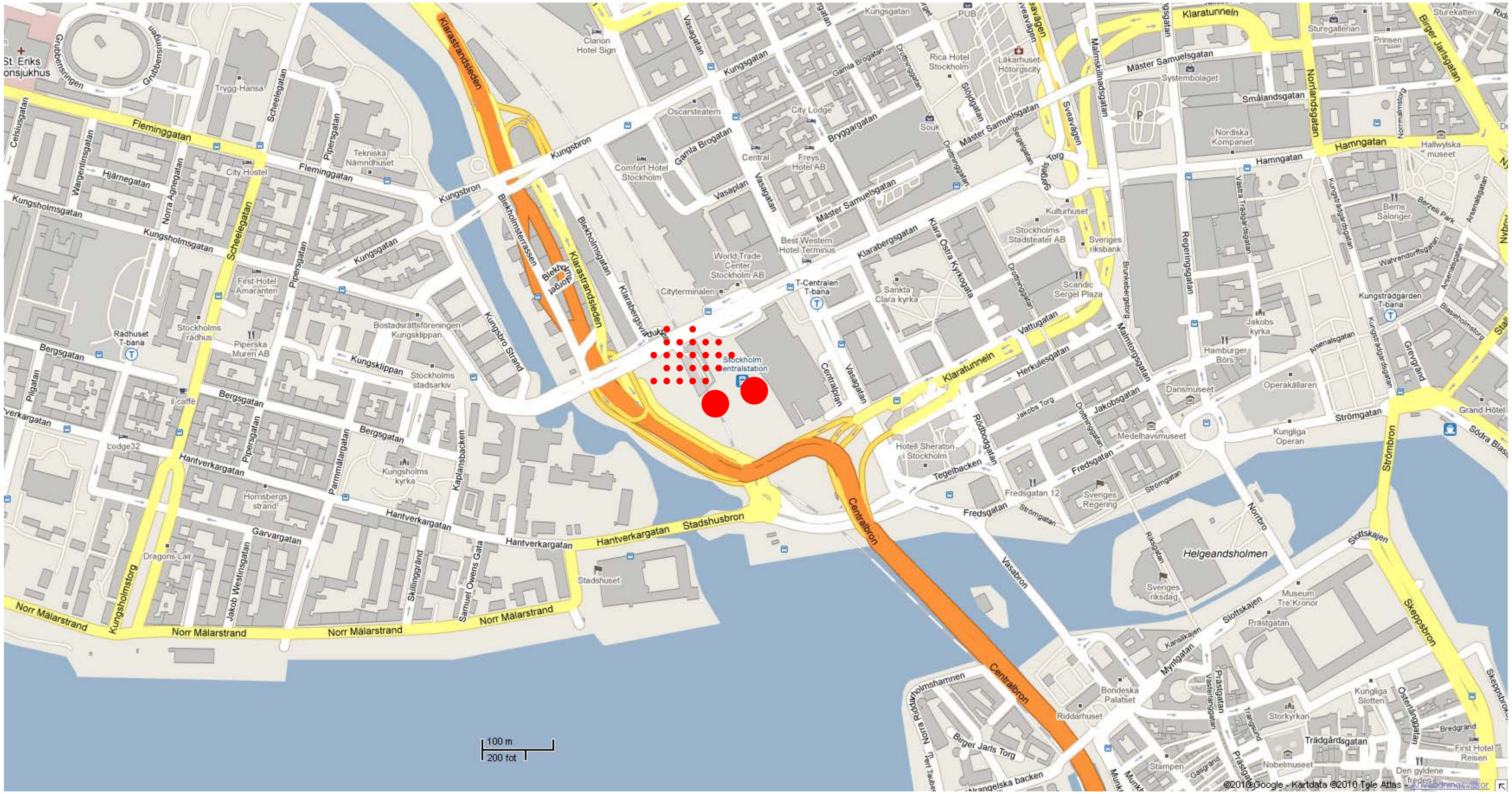
ROYAL INSTITUTE OF TECHNOLOGY

This will be difficult!

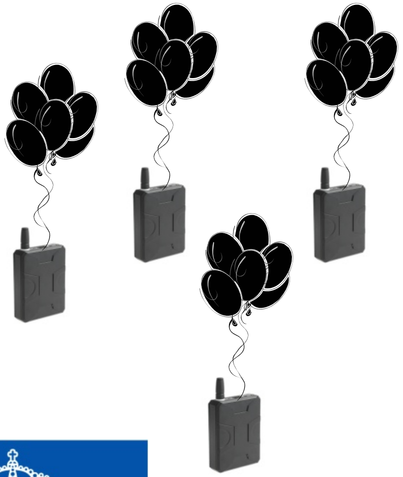


● ≈ 10 m diameter of effective jamming zone.

ROYAL INSTITUTE OF TECHNOLOGY



Concept of “mitigation”



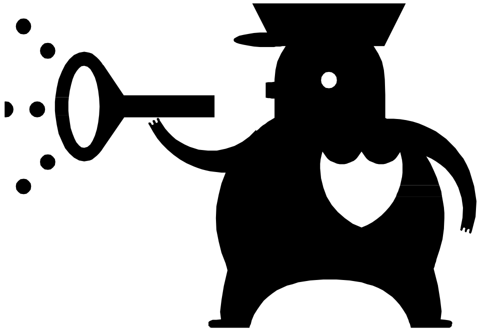
The “mitigation” is based upon inhibiting the interference source. By using a HPEM counter source to create an upset event in the jammers, leading to a stop of their operation.

However, to be “realistic” it is required to use a:

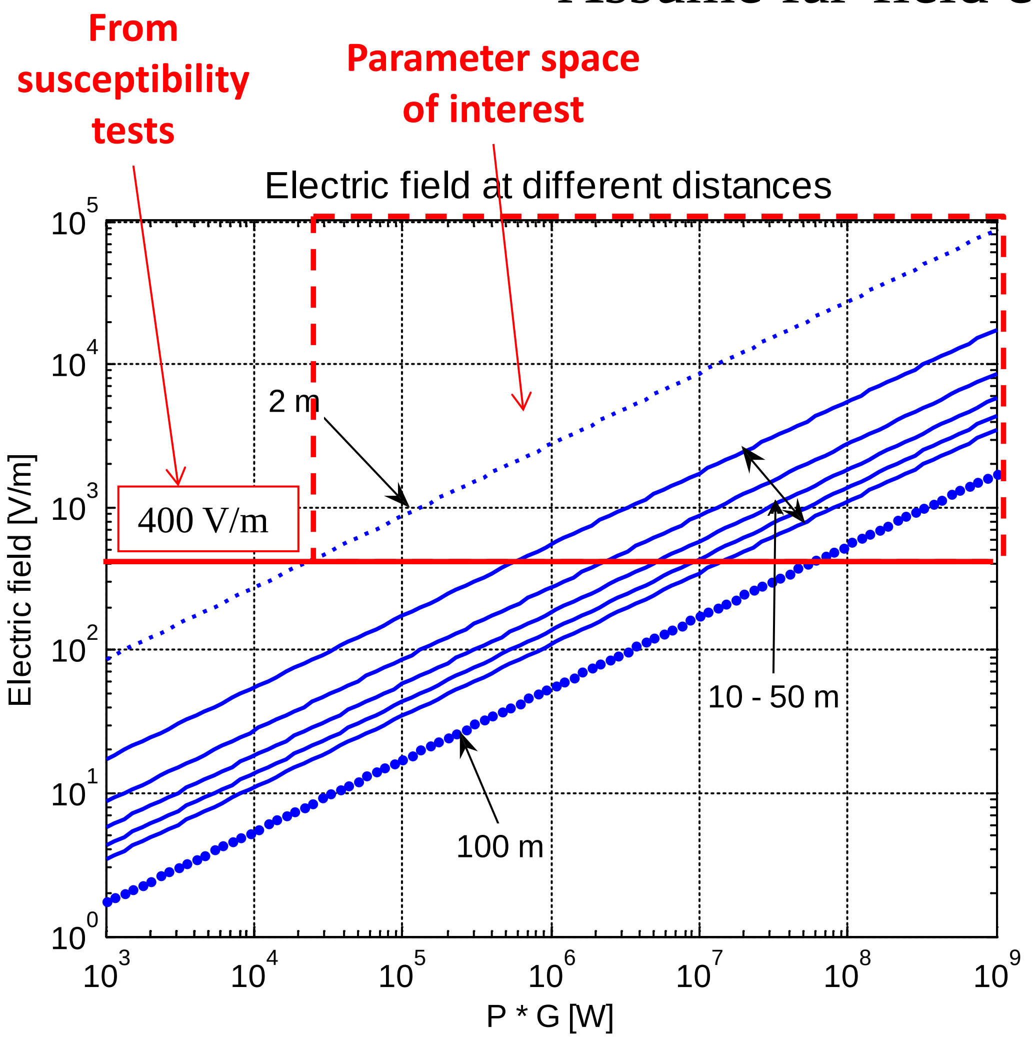
1. “Small” source of robust design.

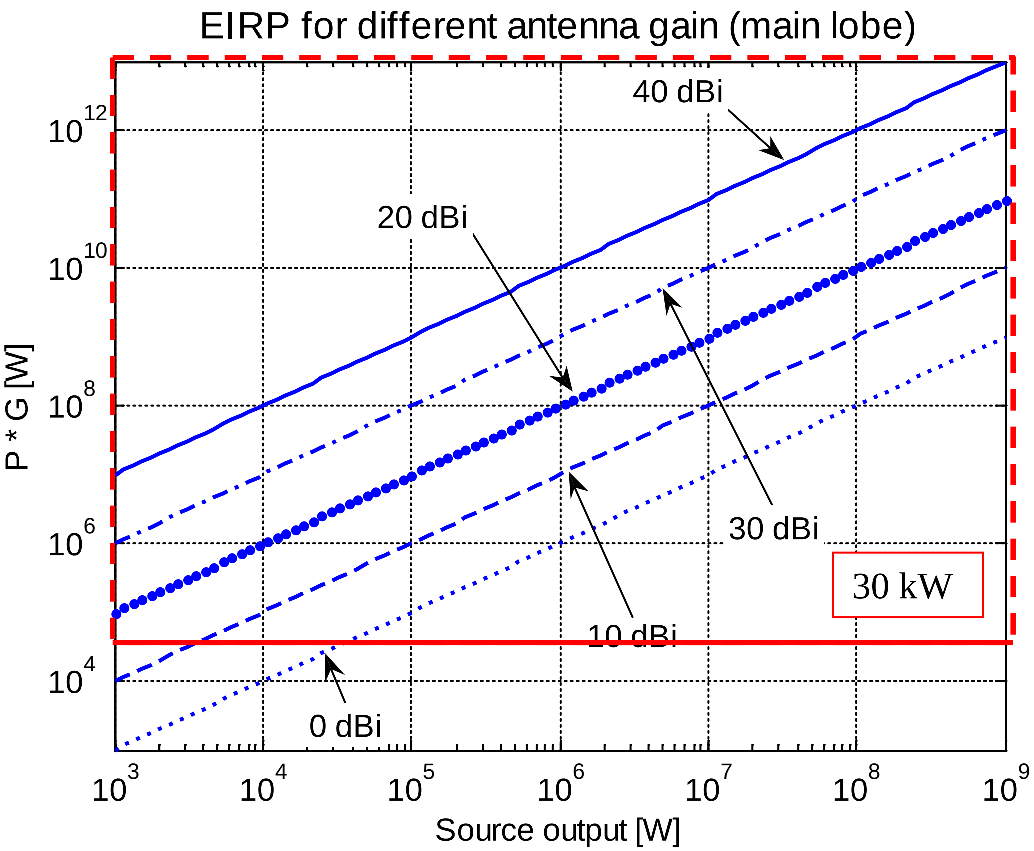
2. “Small” antenna with relatively high directivity (≈pencil beam).

Also, the **effective** operative range of the HPEM counter source should be in the range of [2 : 100] m (distance to jammer).



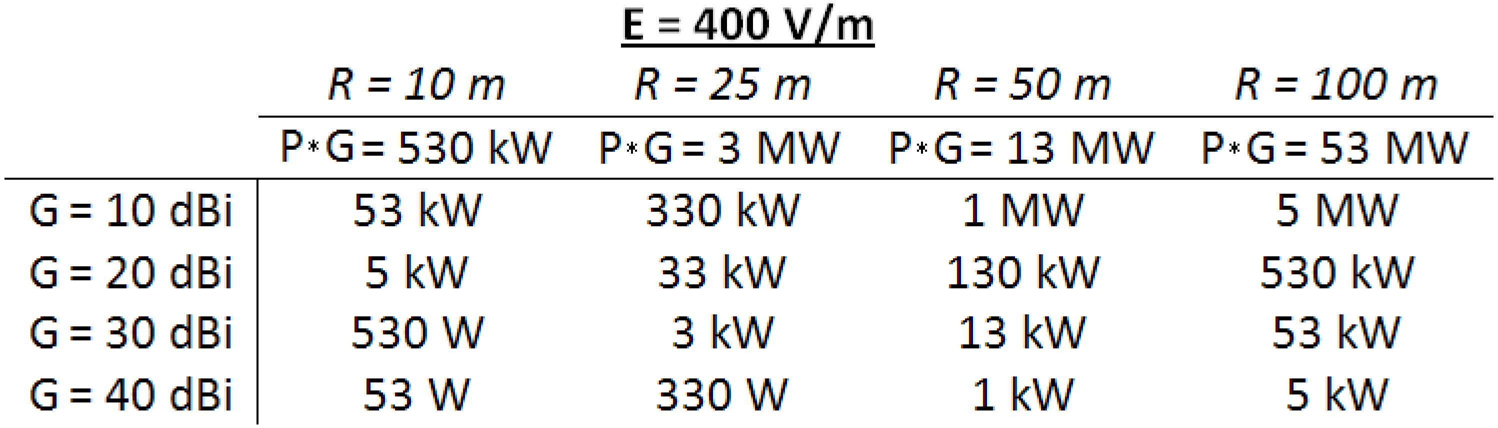
Assume far-field conditions: $E = \frac{\sqrt{30PG}}{R}$





Remember that through conjugate matching the maximum power from source to antenna is given. Only 50% is then feed from source to antenna.

Source output for different cases



E = 400 V/m

	R = 10 m	*R = 25 m*	*R = 50 m*	*R = 100 m*
	P*G = 530 kW	P*G = 3 MW	P*G = 13 MW	P*G = 53 MW
G = 10 dBi	53 kW	330 kW	1 MW	5 MW
G = 20 dBi	5 kW	33 kW	130 kW	530 kW
G = 30 dBi	530 W	3 kW	13 kW	53 kW
G = 40 dBi	53 W	330 W	1 kW	5 kW

ROYAL INSTITUTE OF TECHNOLOGY

Constraints on this are:

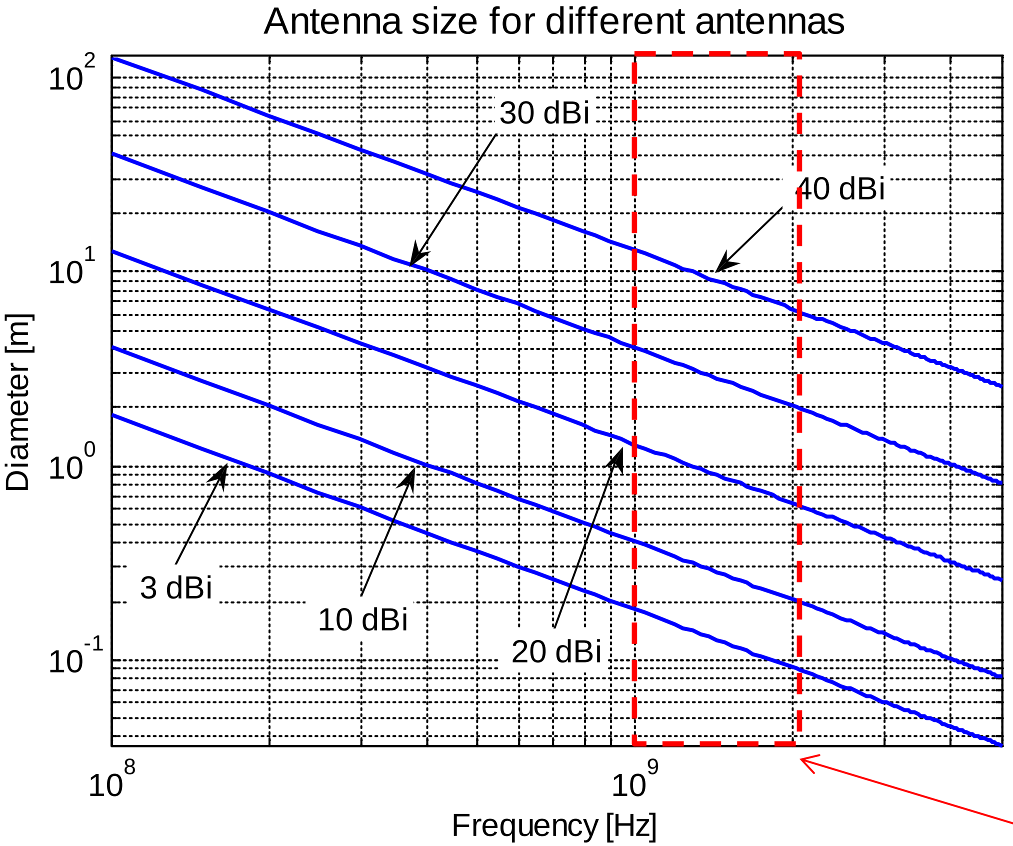
1. Is the assumption of far-field conditions realistic for our considered range interval?
   a. Antenna size?
   b. Distance to far-field?

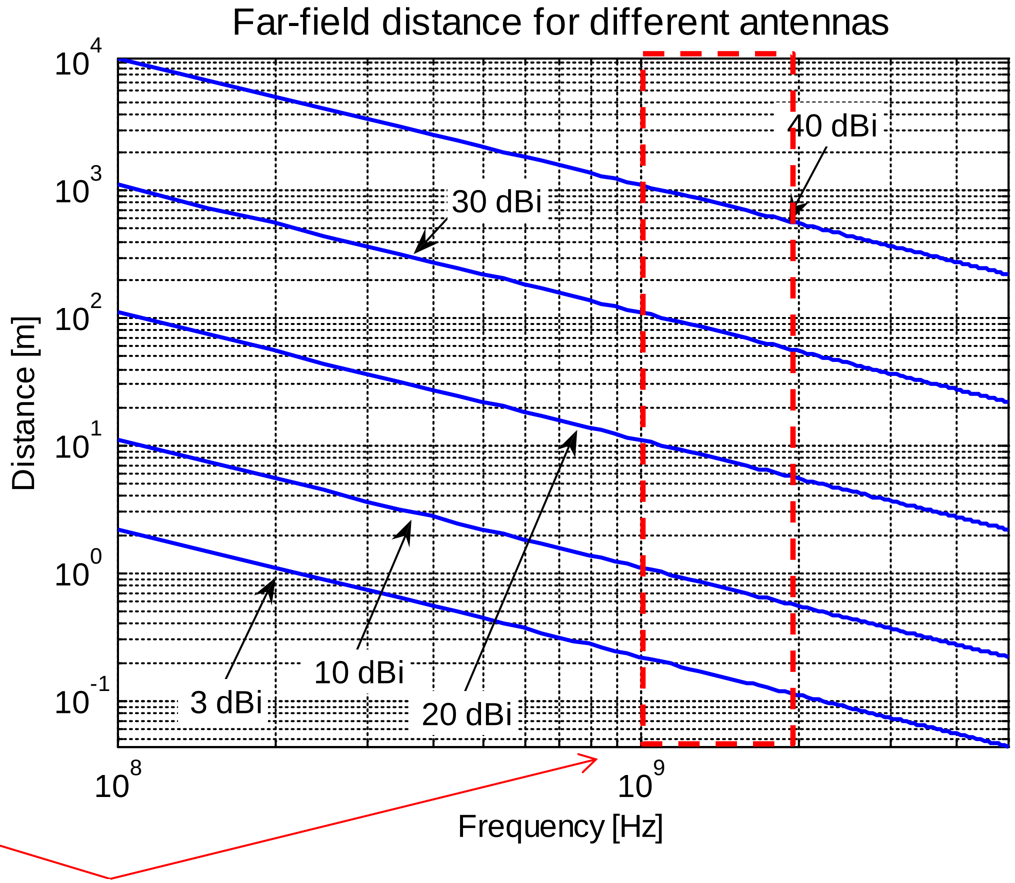
2. Available source and antennas realistic for this operations.

Reflector antenna is assumed (and η= 0.55)

$$D = \frac{4\pi}{\lambda^2} A_{eff} = \frac{4\pi}{\lambda^2}\eta A_{physical}$$

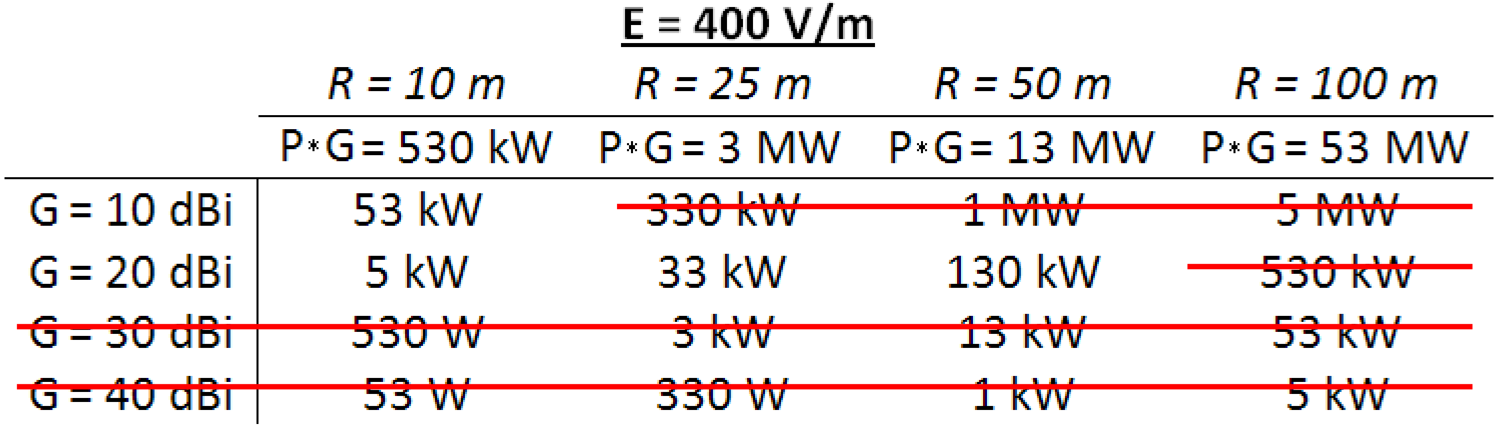
$$\left.\begin{aligned} D &= \frac{4\pi}{\lambda^2}\eta A_{physical} \\ R_{far-field} &= \frac{2Dim_{\max}^2}{\lambda}\end{aligned}\right\} \rightarrow R_{far-field} = \left.\frac{2D\lambda}{\eta\pi^2}\right|_{\max dim}$$





Frequency of jammer and immunity data ≈ [1 : 2] GHz

Source output for different cases



E = 400 V/m

	R = 10 m	*R = 25 m*	*R = 50 m*	*R = 100 m*
	P*G = 530 kW	P*G = 3 MW	P*G = 13 MW	P*G = 53 MW
G = 10 dBi	53 kW	~~330 kW~~	~~1 MW~~	~~5 MW~~
G = 20 dBi	5 kW	33 kW	130 kW	~~530 kW~~
~~G = 30 dBi~~	~~530 W~~	~~3 kW~~	~~13 kW~~	~~53 kW~~
~~G = 40 dBi~~	~~53 W~~	~~330 W~~	~~1 kW~~	~~5 kW~~

✓For 30 and 40 dBi reflector antennas the antenna size and distance to far-field is too large.

✓Source with output power (CW) in excess of ≈ 100 kW are unreasonable for robust and small COTS sources.

✓From this mission parameters can be chosen and a suitable HPEM mitigation source be designed.

Conclusion

- Easily accessible, low cost commercial jammers found through the internet works as specified.
  - However a 3G phone was unaffected.

- The jammers can be interfered with both in- and out-of band EMI of a some 100’s V/m.

- A countermeasure of a HPEM source could be used to induce a Level 4 upset (crash) in the jammer.

Thank you.