

# How to kill UAVs

The UAVs have two alternative systems for communication.

**Line of sight radio :**

In the military C-Band 500 - 1000 MHz that can be jammed with simple spark-gap radio

**Satellite communication :**

In the Ku-Band between 10.95 - 14.5 GHz, and the satellite can be jammed.

The Uplink-Band **to** the satellite is 13.75 - 14.5 GHz

The Downlink-Band **from** the satellite is 10.95 - 12.75 GHz

And you should jam the Uplink frequencies with a jammer directed at the satellite.

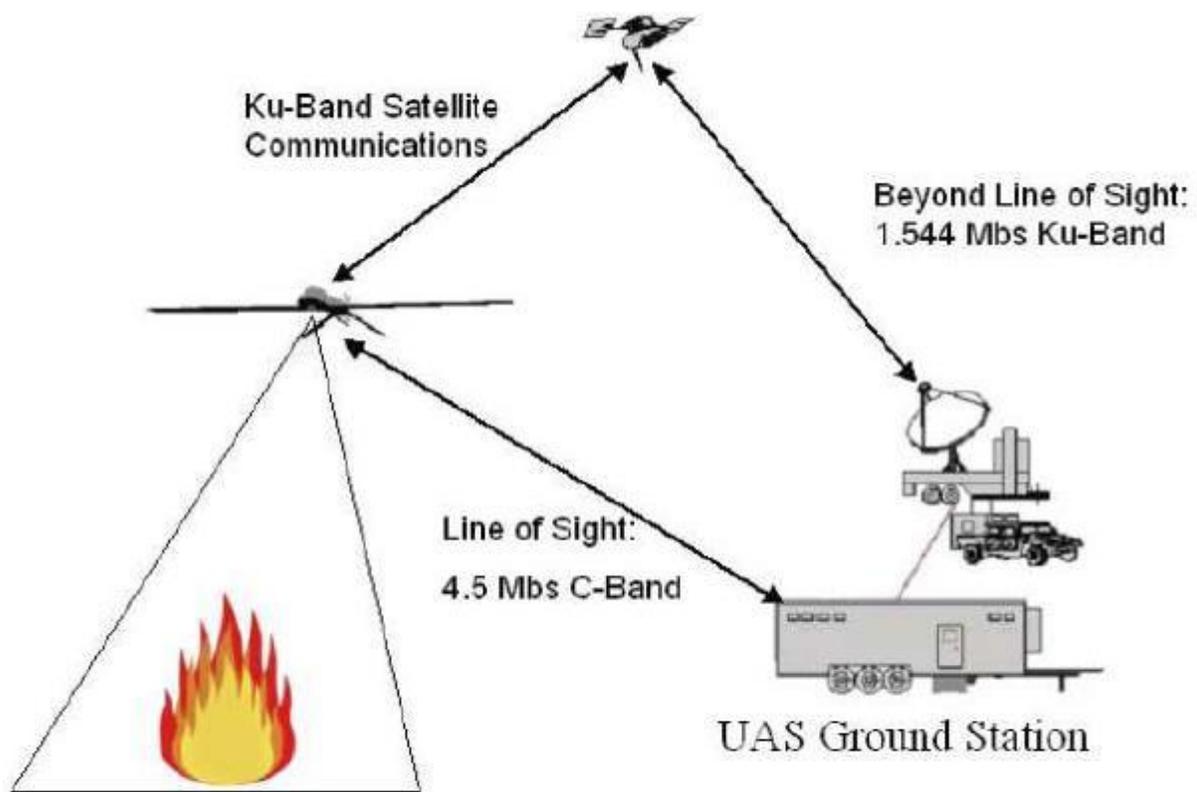


Figure: C-Band and Ku-Band Communication



The satellite link system is from L-3 Communications.  
[Specifications.pdf](#)

Surprisingly, the resistance can tap off the military's video feeds

As you can see in the specifications, the satellite link system uses the same civilian commercial technology as television broadcasting companies. And the surprise is that the resistance and others have tapped off the videos from the battlefield with simple commercial equipment. But now the communication is perhaps encrypted. [Read more about SkyGrabber.pdf](#)

If you jam the communication, then the operator becomes blind and the UAV will fly around until it crashes or the fuel is gone. But you must kill both links of communication to kill any rescue.

There are a limited number of satellite channels available which means that the satellite link becomes a bottleneck. The satellite is therefore used as a backup and jammer-rescue channel and for **single special operations** from far away from the target, while C-band radio is used for multiple simultaneous operations from near the targets. Every military base have their own UAVs that must be operated through the C-band radio. C-band radio is also reported to be used for take off and landing. Which means that **the C-band radio is your primary target**. The C-band radio is also easier to jam.

---

## First some clips from the web

<http://www.lexingtoninstitute.org>

Lack of protected satellite communications could mean defeat for joint force in future war. Defense experts have repeatedly warned that the availability of space-based communications could be compromised in future conflicts by the fact that **80-90% of all military traffic is transmitted on vulnerable commercial satcom channels**. However, there is a related problem that far fewer military observers have noticed: only about 1% of defense communications today are protected against even the most modest jamming threats.

[http://www.abc.net.au/science/news/space/SpaceRepublsh\\_120537.htm](http://www.abc.net.au/science/news/space/SpaceRepublsh_120537.htm)

According to the US Air Force, information from the internet is being used to sabotage satellite signals critical to military operations.

This week's New Scientist reports that instructions on how to build satellite jammers, using cheap equipment from home improvement stores and electronics fairs, are to be found on the internet.

The US Air Force team, dubbed the Space Aggressor Squadron, was set up to look for weak spots in satellite communications and navigation systems by playing the part of a potential enemy.

"We ran a search on the Net and found there's quite a lot of information out there on how to build

and operate satellites but also, unfortunately, on how to jam them," says Tim Marceau, head of the squadron. "Just type in 'satellite communications jamming' and you'll be surprised how many hits you get."

Two rookie engineers from the US Air Force Research Laboratory were ordered to build a jamming system using only a Net connection and whatever they could buy for cash.

For \$7500, the engineers lashed together a mobile ultrahigh-frequency (UHF) high-power noise source that they could use to jam satellite antennas or military UHF receivers. "It's just like turning your radio up louder than someone else's," Marceau says.

The engineers built their home-made jammer using a petrol-driven electricity generator, wood, plastic piping and copper tubing. The amplification and noise-generation electronics were obtained at an electronics enthusiasts "swap meet".

"For very little money and very little sophistication, we found you could muck up communications," says Marceau. Different components could be used to jam other frequencies, such as that of the Global Positioning System.

[http://www.theregister.co.uk/2005/09/23/us\\_deploys\\_sat\\_jamming\\_squads/](http://www.theregister.co.uk/2005/09/23/us_deploys_sat_jamming_squads/)

The US has created electronic-warfare squads capable of jamming enemy satellite transmissions. Fearful of losing its advantage of superior technology resources over its potential enemies

<http://en.wikipedia.org/wiki/Satellite#Jamming>

Due to the low received signal strength of satellite transmissions they are prone to jamming by land-based transmitters. Such jamming is limited to the geographical area within the transmitter's range. GPS satellites are potential targets for jamming, but satellite phone and television signals have also been subjected to jamming. It is trivial to transmit a carrier to a geostationary satellite and thus interfere with any other users of the transponder. It is common on commercial satellite space for earth stations to transmit at the wrong time or on the wrong frequency and dual illuminate the transponder rendering the frequency unusable. Satellite operators now have sophisticated monitoring that enables them to pin point the source of any carrier and manage the transponder space effectively.

<http://www.wnd.com/?pageId=118345>

The U.S. Army is moving forward with a plan to order thousands of radio-frequency-jammer devices to foil improvised explosive devices, even though terrorists' latest attacks in the Afghanistan war have used mechanical, rather than radio, detonators, according to a report from Joseph Farah's G2 Bulletin.

**The jammers likely will cause problems with remotely operated aerial drones, . . .**

According to experts, U.S. troops experienced jamming **in Iraq in 2006 when the Warlock RF jamming system had a detrimental effect on their communications systems and UAVs.**

<http://www.military.com/features/0,15240,108934,00.html>

**Warlock radio frequency jammers in use in Iraq interfere with Army radio communications and block controls needed to operate unmanned aerial vehicles**, according to a study of the service's initial effort to transform divisions into “modular” brigades.

---

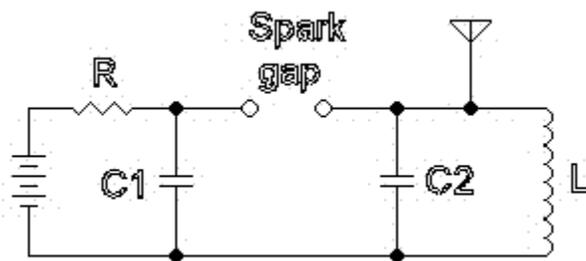
## Spark gap transmitter

The radio pioneers in the old days had no semiconductors or vacuum tubes. And that's the type of transmitter you are looking for if you want to build a jammer at home in your garage.

Every resonant device, a bell or an electronic circuit works in the same manner. Hit the bell with hammer and it will ring for a while. If you repeat the hammering periodically then the bell will ring continuously.

For an electric circuit we should use an electric spark instead of a hammer to do the job.

[http://en.wikipedia.org/wiki/Spark-gap\\_transmitter](http://en.wikipedia.org/wiki/Spark-gap_transmitter)



The coil L and the capacitor C2 is the resonant circuit.

The energy from a high voltage source is stored in the capacitor C1, and is released on every spark. And that makes the resonant circuit ring.

This circuit will then wait for the capacitor C1 to charge up again through the resistor R, and then release another spark. And the spark frequency is about  $1 / R * C1$

For UHF frequencies the antenna itself is the resonant circuit, tuned to a frequency.

The spark gap transmitter has an output power of wide bandwidth, but centered around the resonant frequency. And in case you want to spread out the power more uniformly then try a motorized or electro-mechanical modulation at C2 or the antenna itself. Or multiple transmitters tuned to different frequencies.

**A radio jammer can also be used to deny the enemy to call in air support when you attack. Send out a team to jam the airbase radio before you attack**

**any of those spread out tiny outposts or patrols.**

This is probably what you are looking for

[US patent 4491842](#)

<http://www.freepatentsonline.com/4491842.html>

US military radio jammer that can be used in the military C-Band 500 - 1000 MHz  
It's not necessary to transmit 100 kWatts of power to jam an UAV which means that the construction can be simplified. And you can use a simplified spark-gap.

### High voltage

The high voltage can be generated from a 12 volt car battery in the same way that high voltage is generated to the car's spark plugs. You need a coil and an oscillator circuit that turn on and off a transistor switch. Connect a high voltage diode from the coil to a high voltage reservoir capacitor.

You can also use a motorized electro-mechanical switch.

The only trouble is that you must keep in mind that the capacitors and the coil can be destroyed from overvoltage. Which means that you must somehow turn off the switch if the voltage becomes too high.

But very often the circuit (spark gap) will control the voltage balance itself if it is correctly dimensioned.

### Groundplane reflection

As you perhaps know, you can reach and jam receivers at longer distance away if you put your C-Band transmitter antenna as high up as possible. (don't care with paraboles)

This is caused by the fact that the radiowaves travel two separate ways from your transmitter.

A direct way through air.

And a damped and **phase inverted reflected way, bouncing from the ground.** Which cancels out most of the power from your transmitter.

This damping of your transmitters power can be avoided if you put the transmitter antenna high up.

And also try get as good electric ground connection as possible for your transmitter.

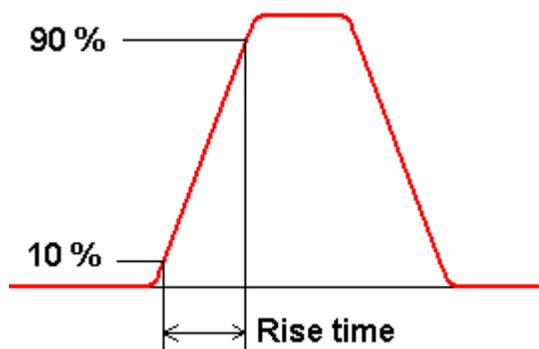
If you connect the antennas through a shielded coaxial cable from a bunker at a safe distance then it becomes almost impossible to destroy the jammer with homing missiles, and too easy to repair a piece of cheap bent metal antenna.

## Spark gap jammer at 14 Giga Hertz frequency ?

This is more complicated but possible and under evaluation by the scientists for use as UWB radar.

And you must improve the spark's rise time in order to make it generate more power at higher frequencies.

### Definition of rise time



There is a simple thumb rule for the relationship between **rise time** and **bandwidth** for spark-gaps and single stage RC filters and oscilloscopes. [http://en.wikipedia/wiki/Rise\\_time](http://en.wikipedia/wiki/Rise_time)

### **Bandwidth \* Rise Time = 0.35**

50 pS rise time will give a bandwidth of 7GHz

25 pS rise time will give a bandwidth of 14 GHz

But you must keep in mind that the upper Bandwidth limit is defined as the frequency at which the power is damped -3dB. **But still there is power emitted at higher frequencies**, but damped. As you can read in the links below power is generated and measured at 5 GHz for a switch with 200 pS rise time. But the thumb rule above says that the Bandwidth is only 1.75 GHz.

These spark gaps can generate GigaWatt pulses which means that you can tolerate the bad efficiency at 14 GHz in your home built jammer.

But since you are building a jammer, not an UWB radar, do you have to change the construction to emit 10-100 times more pulses of (1/1000) less power, with a mean value power consumption of perhaps 100W-10kW.

No guarantee for that the satellite jammer will work in the Ku-Band, but it's simple and worth some testing.

## Fast Rise Time Switch

Two different techniques can be used in your homebuilt jammer.

Electro-mechanical, for example a mercury filled reed relay that can switch with a rise time below 70 pS as you can read in the links below. Or perhaps try a motorized switch ?

High pressure cascaded hydrogen spark gaps that can switch with a rise time below 50 pS.

A spark gap has a static arcing voltage that is lower than the dynamic arcing voltage.

Which means that if you feed a spark gap with a very fast rising voltage then it will take some time before the spark gap reacts. And you can make it arc at voltages that are about 25 times higher than the static arcing voltage. This overvoltage have the effect that the rise time becomes shorter.

And you can improve the rise time by **cascading multiple spark-gaps**.

But keep in mind to optically shield the spark-gaps from each other because the UV light from a spark can turn on the other spark gaps.

If the spark gap is in an extremely high pressure hydrogen atmosphere then it becomes faster.

Up to 125 atmospheres over pressure have been tested by the scientists as you can read, and it looks like the rise time is near an inverse cubic root function of the pressure.

$$t = K / \text{CubicRoot}(\text{pressure})$$

And the electrodes should have no sharp edges.

This has perhaps never been tested ?

Aluminum can emit electrons if illuminated with UV light

And how that affects the rise time is worth some experimenting, if it's possible to create an improved chain reaction with two aluminum mirror electrodes.

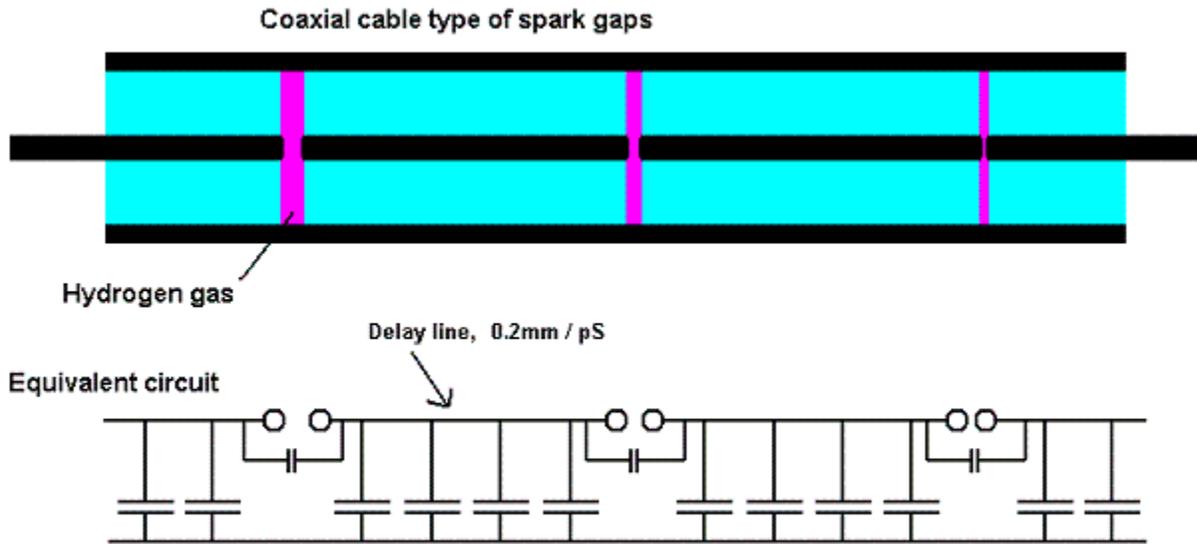
But the life time of the switch is also affected if you use aluminum instead of a heavy metal like copper or tungsten/wolfram. And perhaps aluminum is too soft and will kill the switch with aluminum dust between the electrodes. It may work or not.

## Coaxial cable type of spark-gap

At GigaHertz frequency it becomes hard to keep the radiation under control because every tiny part of the circuit is like an antenna and the radiowaves behaves like light bouncing on everything. You also want to keep the "cable" impedance constant in order to minimize power lost through reflections.

A simple solution is to design the spark-gaps to look like a coaxial cable. Maybe some holes to help the hydrogen gas circulate and be exchanged from an external container. And try build the

spark-gaps and the microwave feed-horn together in the same unit.



It's hard to analyze, but I think that the cable capacitances and the delay lines help fire the spark-gaps in the right order, from the left to the right. The capacitance in the spark-gap itself is small compared to the cable capacitance. Try speculate about how a shorter or longer cable between each spark-gap will change the firing of the spark-gaps. And if any resistors are necessary for discharging of insulated capacitances ?

The impedance of a coaxial cable is a function of relative dimensions and the dielectricum (insulator) used. Very easy to calculate. It's almost only mechanical work to build the jammer. The right side pin is the antenna pin in the feed-horn. But the question is how to connect it in order to discharge all the reservoir capacitances. It can't be hanging in the air. It must be connected to ground somewhere inside the feed horn.

And you must also try analyze how the length of each coaxial section affects the output through reflections and standing waves. Especially the last section.

### Evaluation of your homebuilt jammer

Use your Ku-Band satellite TV system to test your jammer.

Aim the jammer against the satellite.

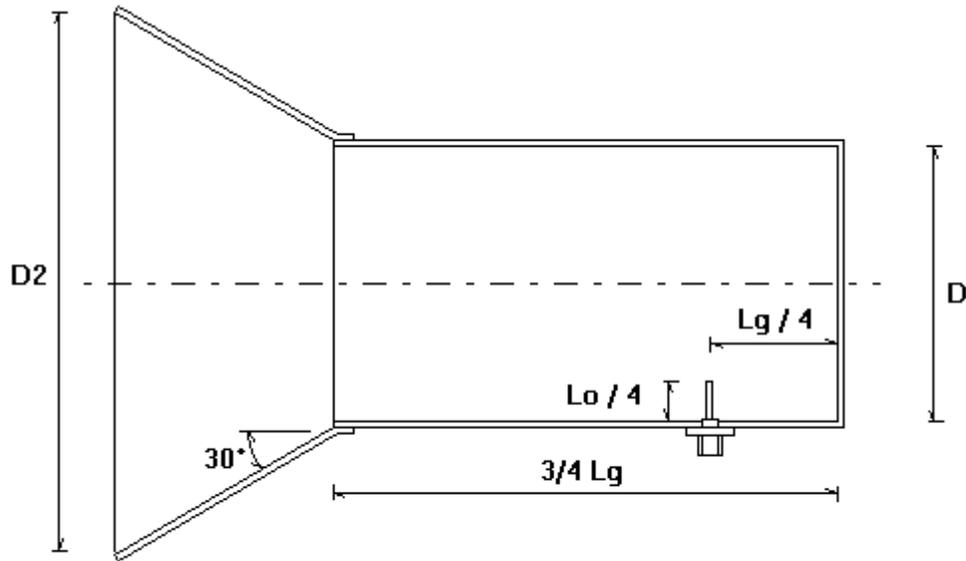
If the TV picture becomes jammed then your jammer works perfectly and is ready to kill the UAV communication.

Also try turn the jammer 90 degrees because the satellite channel can have different vertical or horizontal polarization.

You can also use your satellite TV receiver to low power test your mechanical switch jammers if you put them on a stick and in front of your satellite dish which is aimed at your TV satellite. If you can see any disturbance on your TV screen then it's OK to go to next step, highpower aimed

at the satellite.

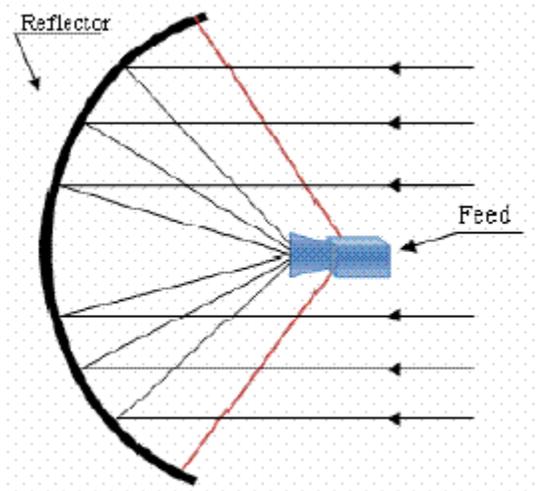
### Feed horn



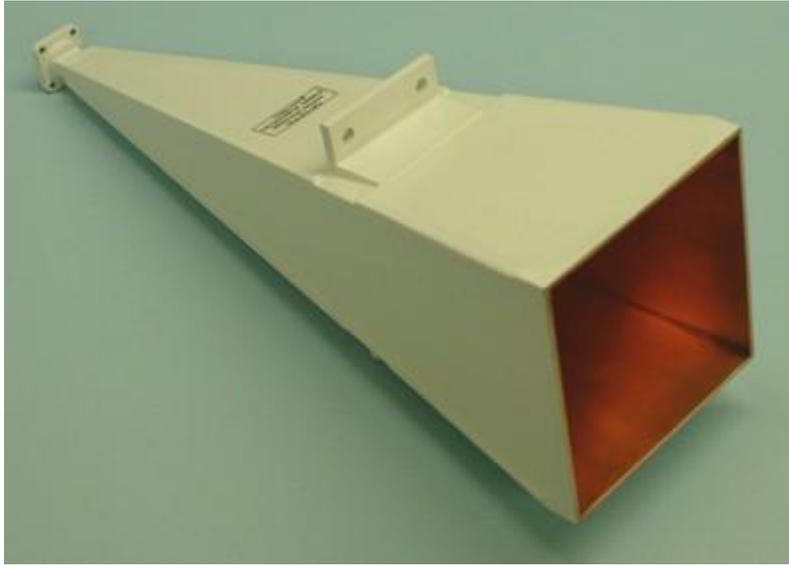
The construction above is from a homebuilt "CanTenna" for 2.4GHz, that can be used as a feed horn to a parabolic antenna.

And you can use the same construction for your jammer at 14 GHz if you change the size.

Note the tiny antenna pin mounted on top of the coaxial cable connector.



Take the parable from a satellite TV system.



Horn antennas have been used for long time to send and receive microwaves. It's a simple construction, but the parabole is more effective if you want higher gain. And want to focus the output power in a narrower beam.

## Some more clips

...Ultrafast gas breakdown under the extreme overvoltages which occur when a high pressure switch is pulse charged to hundreds of KV in 1 ns or less. The highly overvolted peaking gaps produce powerful electromagnetic pulses with risetimes  $< 100$  pS which can be used for ultrawideband radar systems. . . We have produced and accurately measured pulses with 50 to 100 pS risetimes to peak levels of 75 to 160 kV at pulse repetition frequencies (PRF) to 1 kHz.

**Typically the highest pressure with the shortest gap spacing produces the fastest output rise time and minimum switch loss.**

Hydrogen gas is used in e.g radar thyratrons where a current pulse with very steep flanks is desired, since in hydrogen the build-up and the recovery time are much shorter than in other gases.

[http://en.wikipedia.org/wiki/Gas-filled\\_tube](http://en.wikipedia.org/wiki/Gas-filled_tube)

Hydrogen is used in tubes used for very fast switching, e.g. some thyratrons, dekatrons, and krytrons, where very steep edges are required. The build-up and recovery times of hydrogen are

much shorter than in other gases.

Collected documents from the web :

[10353.pdf](#)

Compact high-voltage picosecond generator used as pulsar transient radar source

[1650709.pdf](#)

Ultrafast gas switching experiments

[slac\\_pub\\_4858.pdf](#)

High speed switching in gases.

[ssn480.pdf](#)

A highly directive, very intensive, impulse like radiator. UWB Ultra Wide Band

[539554.pdf](#)

Picosecond high pressure gas switch experiment.

[31295012202627.pdf](#)

High voltage subnanosecond dielectric breakdown

[Ljp49105.pdf](#)

Radiation of ultra-wideband electromagnetic pulses by pulsed excitation of rectangular antenna.

Links :

**Homebuilt CanTennas for 2.4 GHz**

<http://www.turnpoint.net/wireless/cantennahowto.html>

<http://www.saunalahti.fi/elep/antenna2.html>

<http://www.wlan.org.uk/antenna-page.html>

**70 pS rise time pulse generator that uses a mercury filled reed relay**

[http://www.fkh.ch/pdf\\_files/Pulsgen.pdf](http://www.fkh.ch/pdf_files/Pulsgen.pdf) alternative [Pulsgen.pdf](#)

100 pS

<http://www.dtic.mil/cgi-bin/. . . .GetTRDoc.pdf> alternative [GetTRDoc.pdf](#)

### **Horn antennas**

[http://www.ramayas.com/Horn\\_Antennas.htm](http://www.ramayas.com/Horn_Antennas.htm)

<http://www.w1ghz.org/antbook/chap2.pdf> alternative [chap2.pdf](#)

<http://www.ets-lindgren.com/page/?i=RFAntennas>

<http://www.ijetch.org/papers/013.pdf> alternative [013.pdf](#)

<http://www.q-par.com/products/horn-antennas>

<http://www.qsl.net/n1bwt/contents.htm>

### **Satellite information**

<http://www.lyngsat.com/launches/ku.html>

---

## Jam the satellite with commercial equipment

Any television station with an uplink can jam a satellite. All it takes is two uplinks trying to broadcast at the same time

As you can see in the specifications the military use the same technique as the commercial TV channels. And the UAV's output power is only 50 Watts.

All you have to do is to jam the satellite with your own transmitter.

Satellite communication systems use a device named TRAVELING WAVE TUBE TWT to amplify microwave frequencies. [http://en.wikipedia.org/wiki/Traveling-wave\\_tube](http://en.wikipedia.org/wiki/Traveling-wave_tube)

Even if simple in construction, these are usually nothing that you will build in your garage at home because it is a vacuum tube.

The major manufacturers of TWTS are EMI-Varian, Ferranti, EEV, Hughes, STC, Litton, Raytheon, Siemens, Watkins-Johnson and Thomson-CSF and also some russian and japanese companies.

The TWTs are usually sold and assembled together in a box with all necessary high voltage and control electronics. See picture below.

But you can buy the TWT tube itself as a spare part because it has a limited life time, like a

lamp.

The TWT is an amplifier (not an oscillator) and doesn't generate any output frequencies if it has no input signal. And you need more equipment.

You need this equipment :

- 1 Jammer video signal from perhaps a simple PC video card.
- 2 UHF modulator to convert it to a carrier TV frequency that the UP-converter can accept.
- 3 UP-converter to an adjustable Ku band frequency, or to a block of frequencies.
- 4 TWT equipment for power amplification
- 5 Parabolic antenna

The UP-converter 3 can be of two types, with a single input UHF (TV) channel or a block of UHF input channels, (a block converter.) And if you use a block converter then perhaps can you try connect a home built UHF jammer instead of the video 1 and modulator 2 to the UP converter. That will also kill every channel on the satellite instead of a single channel.

If you can't build or buy this equipment then try steal it from a TV broadcasting company. (In war time noone cares about the law. Steal, kill destroy.)



Rack mounted traveling wave tube equipment.



Block converter

**Some examples of manufacturers :**

<http://www.miteq.com>

[http://www.ar-worldwide.com/html/12210\\_twt\\_amplifier\\_twta.asp](http://www.ar-worldwide.com/html/12210_twt_amplifier_twta.asp)

<http://www.ifi.com/web/html/intro/TWTamplifiers.htm>

Google

<http://www.google.se/search?q=traveling+wave+tube+twt>

Happy experimenting, and killing of UAVs

[HOME](#)