The IED Problem

A Study

Contents:

Chapter 1

Problem Definition – Threat Analysis

"If you know the enemy and know yourself, you need not fear the result of a hundred battles.
If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself, you will succumb in every battle."
- SUN TZU ON THE ART OF WAR

According to ***Ref. 1*** over 300 US and coalition soldiers killed or wounded from Improvised Explosion Devices (IEDs) in a short period of time. IEDs are hidden roadside where military convoys drive by. An observer, located at a safe distance, transmits a command triggering the IED at the appropriate time.

The damage caused depends generally on the number of IEDs emplaced, the explosive type and blast power, the armature of the convoy vehicles and speed of travel, the spacing between the convoy vehicles and the IED distance from the convoy at the moment of explosion. The last is also a function of the observer reaction speed, his remote control system speed of transmitting the detonating command, the length of that command, the detonator-explosive delay and it is also a function of the observer safety distance if transmission propagation time periods would be taken into account into a geometry model like the one shown in ***Fig. 1***.

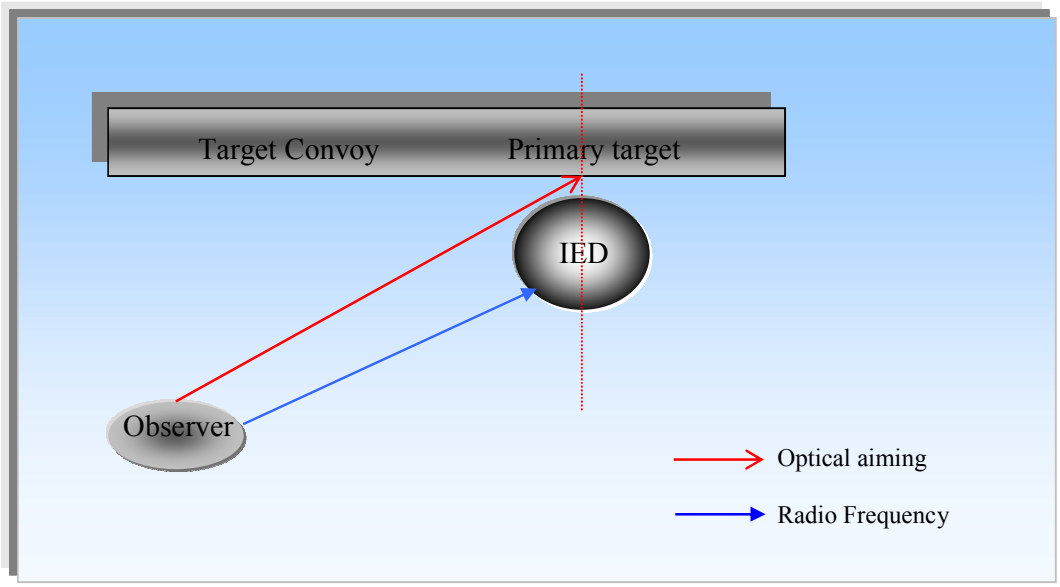


Fig. 1. *The "IED system" includes the IED ellipse, which contains explosives, a remote control receiver with an antenna and a battery, and also includes an observer (standing-off) who first aims at the target optically and then triggers the IED using RF. The observer – operator entity is an IED system requirement, because it is assumed that there are no other sensors and processing that would automatically trigger the IED on time.*

An RF remote control system is assumed in this paper. The use of wireless devices provides the observer with the added benefit of mobility, for example he could change his location in order not to be seen or attract attention, while keeping his viewing field together with his safety distance. Also, the use of RF wireless systems today is inexpensive and wireless devices are easily obtained from the commercial market. The wide range of different commercial wireless systems makes any countermeasures difficult or incomplete and this also adds to the IED benefits. For example, a person seen to be talking to his cell-phone does not attract attention but this person could be the observer that would be transmitting the detonating command to the IED. A garage-door opener or a radio controlled child-toy (sometimes they are called junk-frequency devices) is much more inexpensive and widely available and could be hidden in the observer's pocket with the added benefit that such a device

does not rely on cell-phone network availability or traffic (it is network-independent), while it is readily equipped with a primitive, at least, protocol required for a valid detonation transmission.

The IED detonation transmission protocol in general is assumed in this paper to be required by the IED system, because the observer needs to have as much control as possible over the transmission. Obviously, a remote controlled receiver that would activate the IED by chance (interference, other local wireless use etc.) is not fully desirable and a receiver or a number of receivers that would activate the IED only when a "quick" and "valid" command has been transmitted is required. The words quick and valid calls up for a protocol requirement and highly sophisticated protocols are already available today in the commercial remote control systems in order to add in security and privacy.

Mobility is supported by the use of batteries as the power source for such devices both at the IED receiver and the remote transmitter. There are some points under consideration on this subject and are presented later in this paper.

A covert IED is also required. The IED must be hidden or camouflaged so it shouldn't alert the convoy crew of its presence. This requirement leads the IED operator to choose a remote control operating at higher frequencies (VHF and up) in order to keep the associated antennae short in length. However, the use of lower than VHF range frequencies is not improbable.

In order for an IED to be hidden easily, its volume should be kept low. Considering the volume of the explosives, the added volume of the remote control receiver, its antenna and battery should also be kept low. Here, higher frequency devices with lower power consumption are preferable.

In order for an IED to be emplaced in a position and then wait for the detonation command when a convoy will pass, with a continuously working receiver, batteries capacity is an issue. Increased capacity means increased battery volume. A high-volume discharging-battery may be an active source for a chemical detection based countermeasures device. But considering that the IED users place the explosives in a known or regular - casual convoy route then there is a possibility for the battery to be small enough to be undetectable.

The human factor should also be considered because it affects the technical discussion. It includes:

HF1. The observer's reaction time as mentioned above, because the observer's brain (as part of the IED system) selects the target and calculates the exact instant of "pressing the button" while the convoy is passing. This time is in the order of milliseconds.
HF2. His decisions or reactions in the possibility of civilians or friendly individuals are in close proximity to the IED at the "wrong" time.
HF3. His reaction in the possibility of, because of countermeasures, the IED wouldn't operate as planned.

In an hypothetic countermeasure system that "senses" the presence of explosives in close proximity to the convoy the time in HF1 adds to the time available for calculating the decision of activating a jammer to prevent the receiver from receiving the detonating command from the observer's transmitter or activating an EMP weapon to destroy the electronics of the receiver and this time adds to the radio propagation times in the geometry model. Here the convoy has the "advantage" of being placed very close to the IED, while moving towards to the IED and when it is next to the IED and this improves its capability to detect any radiation coming from the IED and improves its jamming effectiveness as well. In the case of a countermeasures system that would first detect and identify the transmitted command coming from the observer's transmitter and quickly activates the jammer to prevent the IED's receiver from getting a valid command, then this timing advantage is lost.

About HF2, any countermeasures should be designed in such a way that would reduce the possibility of causing a premature explosion by themselves. If the observer would decide not to activate the IED, the convoy systems should not be forced to do it. Of course, if there were not any protocol in the IED system (e.g. just a carrier operated switch at the IED receiver), then almost any jammer probably would cause a premature explosion.

The HF3 has to do with the type of remote control system used. If for example the IED remote control is a cell-phone, a jammed cell-phone receiver would lost its connection with its network and the observer would probably not activate the IED after the convoy has passed and the convoy jammer does not affect anymore the IED receiver and after the network availability has been recovered. There is enough time at this example before the cell phone is operable again and the convoy would be far away and it is the most logical assumption that the observer would choose not to keep trying to explode the IED. But in the case of a garage-door opener (where there really is a fire-button) the observer most probably should keep his finger continuously on the button while the convoy is passing and the IED would not being exploded because of jamming. This means, exactly after the jammer effectiveness would be decreased, because of the convoy movement away from the IED receiver, a late explosion will occur. However, if the jamming power is high and the effective jamming range is much larger than the convoy area, then the observer may see that a late explosion is senseless.

One more issue affected by the HF3, is that if the observer seeing that the IED is not being exploded, decides to move himself towards the IED, in order to increase his signal power at the receiver of the IED. Then his signal may arrive stronger than the jammer's signal and the explosion will occur. So a well-defined jammer burn-through range is required (See ***Ref.3***).

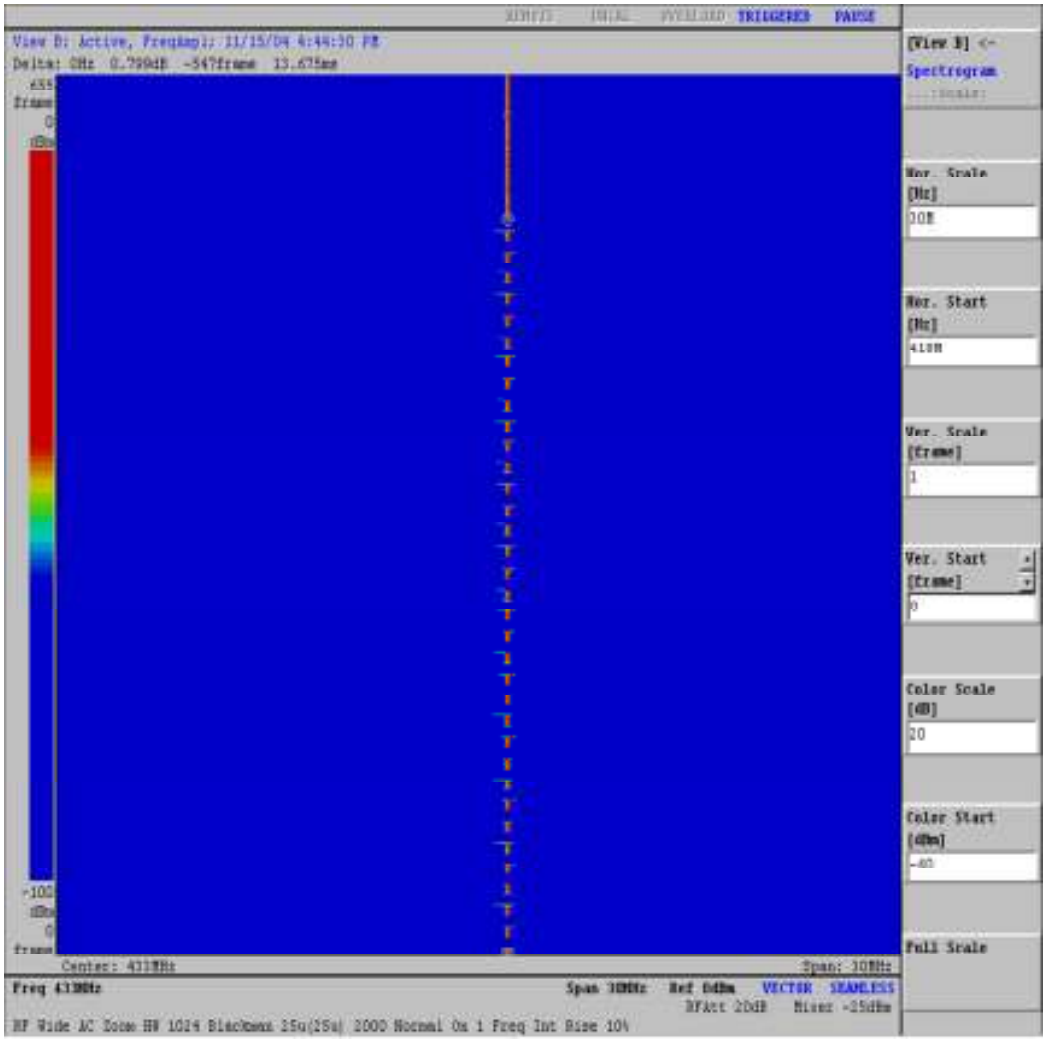
Although a number of commercial equipment could assemble a basic low-cost IED system, its performance should not be under-estimated in the study of a countermeasures device. For example, car-lock remote controls and car-alarm remote controls are very sophisticated to prevent car thieves from un-locking and operating passenger cars and to prevent all the other individual same-model owners from ID coding mess. They represent a very good example of a "suitable" protocol for a quick and valid IED detonating command transmission. They are considered of being short-range devices (approx. 20 meters range) but with the addition of a simple short wire

acting as an external antenna both at the transmitter and at the receiver, turn them to be very powerful with increased range, more than 300 meters.

Relatively the same applies to general-purpose remote controls such as those used as garage-door openers.

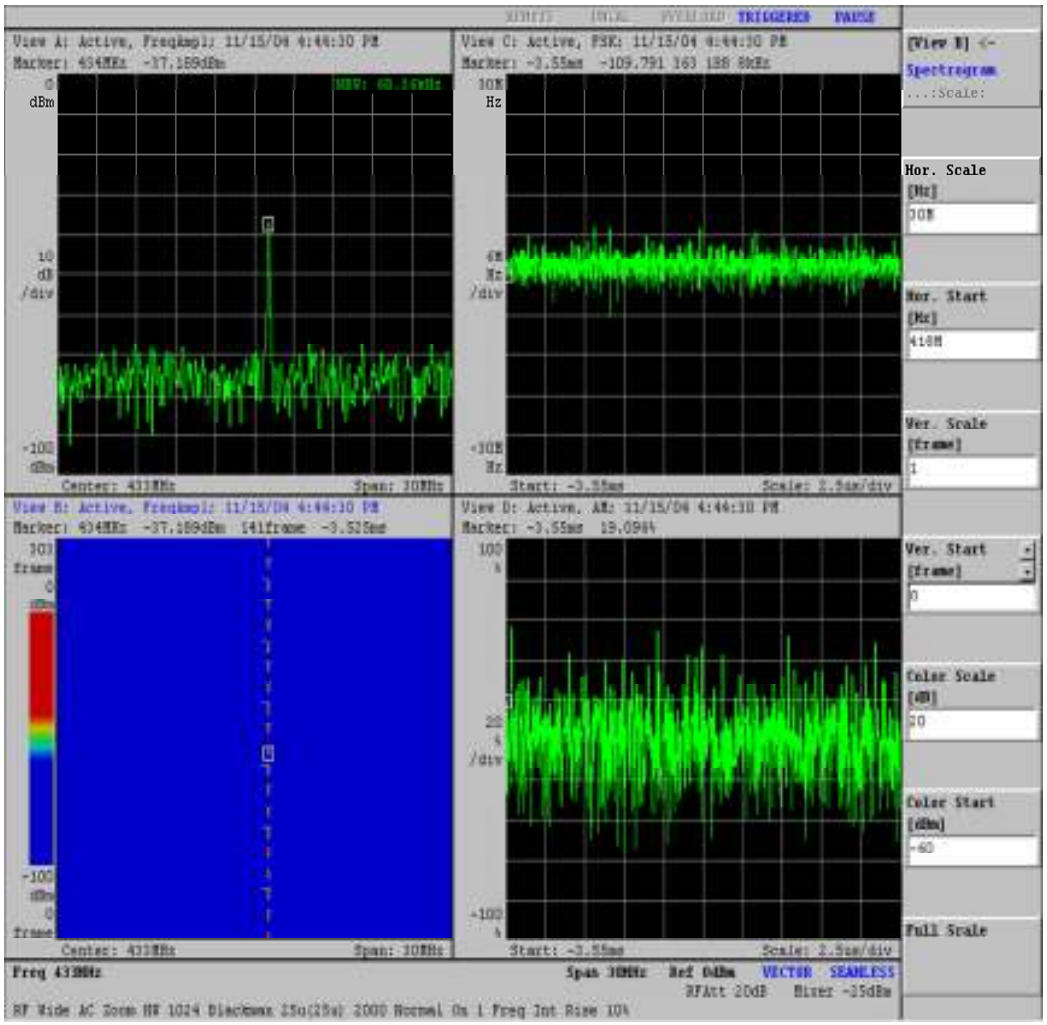
Below, some SIGINT data are given, taken from such devices.

Case 1. *Italian Car Model Alfa Romeo A147 door lock*



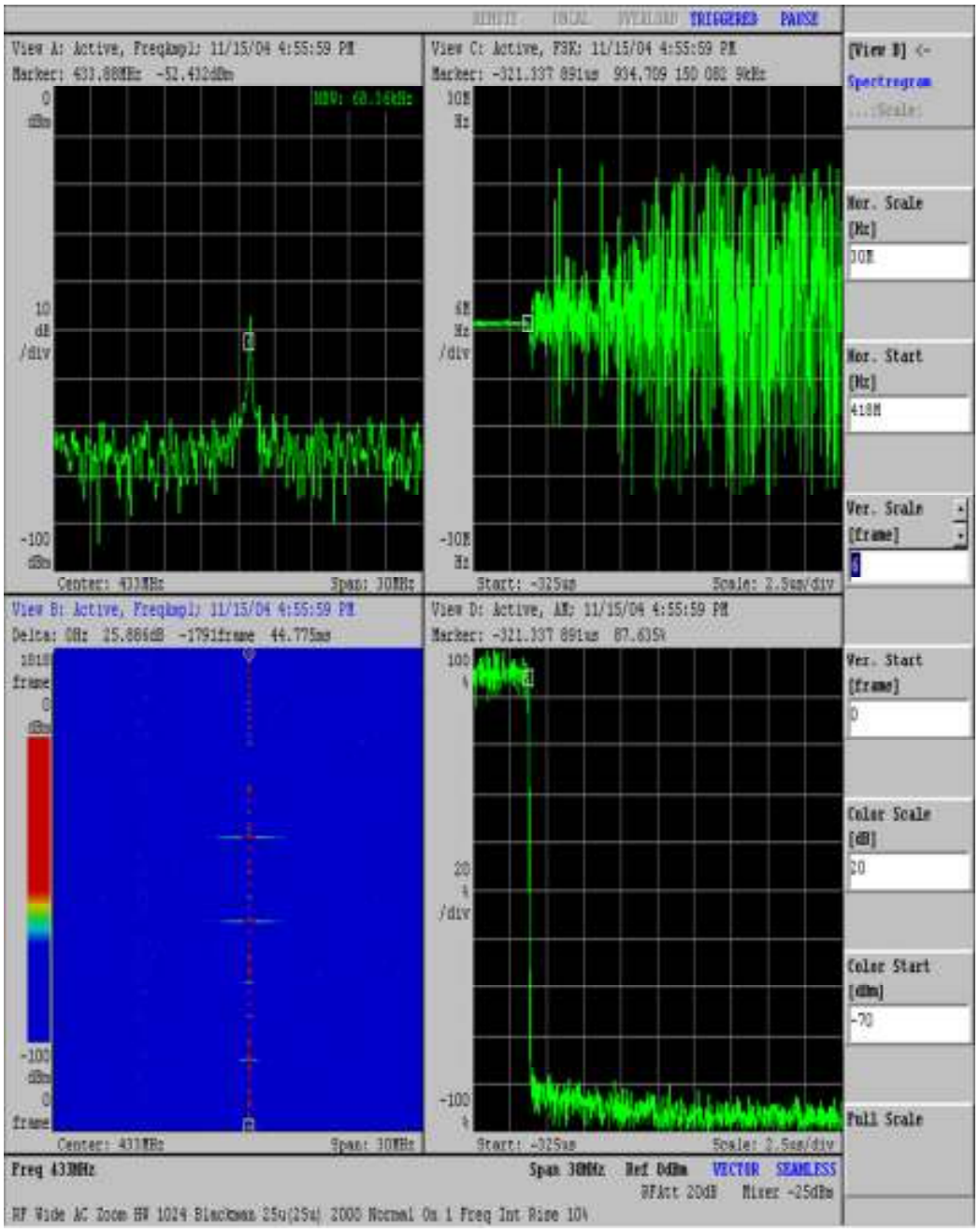
This remote control uses OOK (On-Off Keying) modulation. After a short preamble (at the top of the image), a 13.675 msec long code was sent consisting of 35 pulses of 200 μsec each. The Off interval period was also 200 μsec. It is simple but quite short.

Case 1. - Cont.



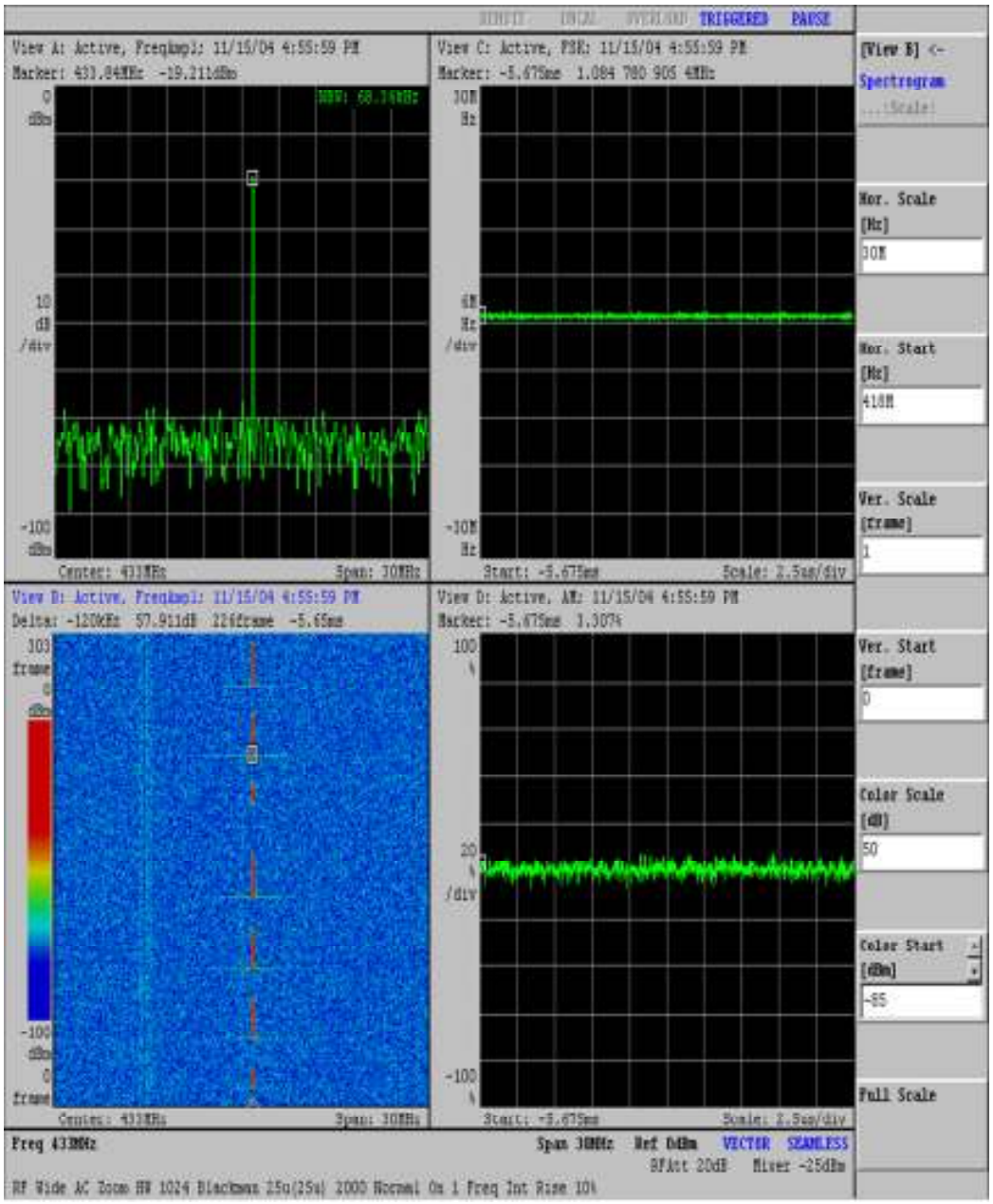
The signal frequency is 434 MHZ. No evidence of FM, AM, FSK or PSK modulation. The pulses seen, carry no other modulation, they are CW pulses.

Case 2. *Japanese Car Model Toyota RAV-4 door lock*



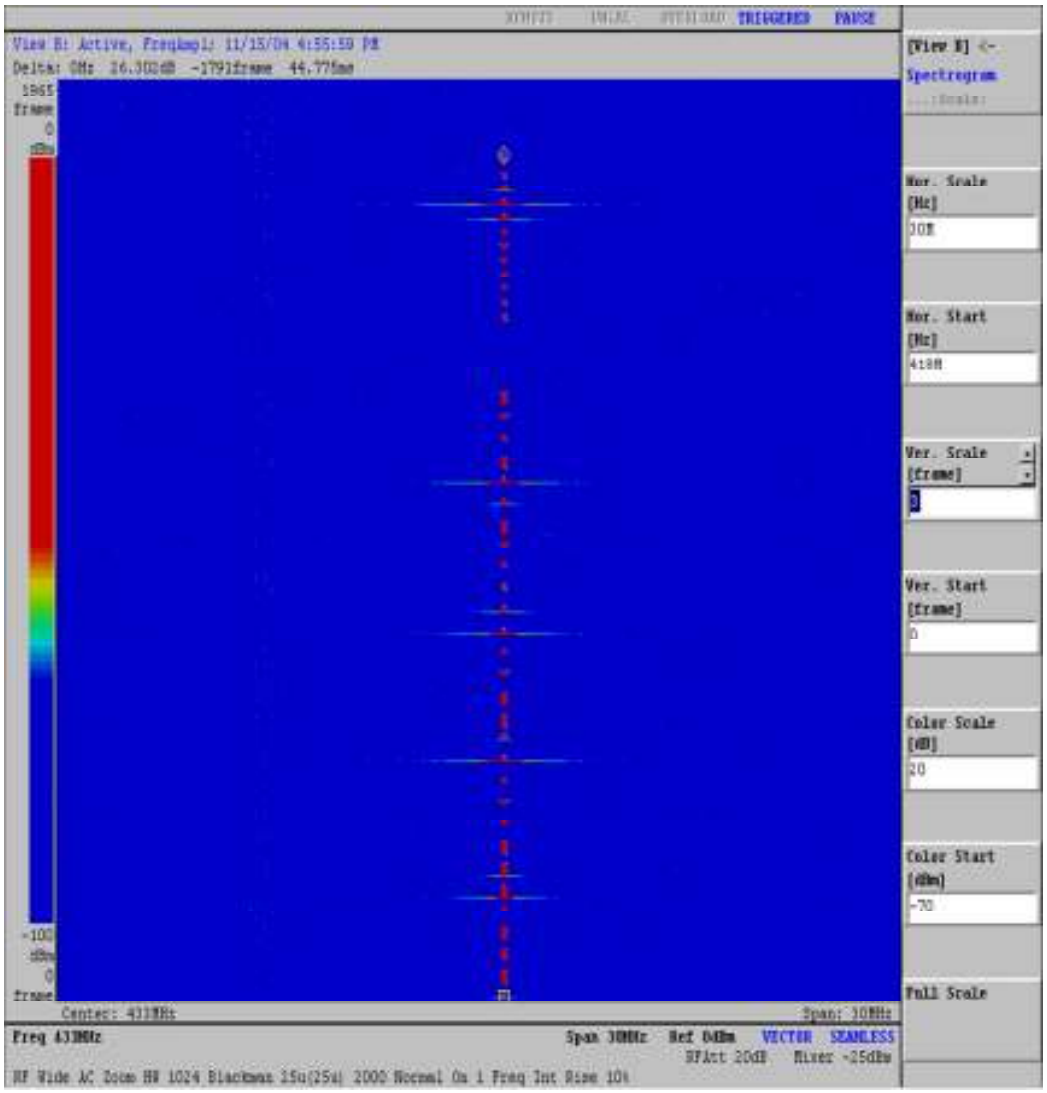
Looks more complicated from Case 1. After a preamble of 12 equal length - equal interval pulses and a short delay, the individual code is send consisting of variable length pulses (Pulse Code Modulation). All of the sequence of pulses lasts for 44.775 msec. The marker is placed at a rising point of a pulse.

Case 2. – Cont.



The signal frequency is 433.840 MHZ. There is CW again.

Case 2. – Cont.

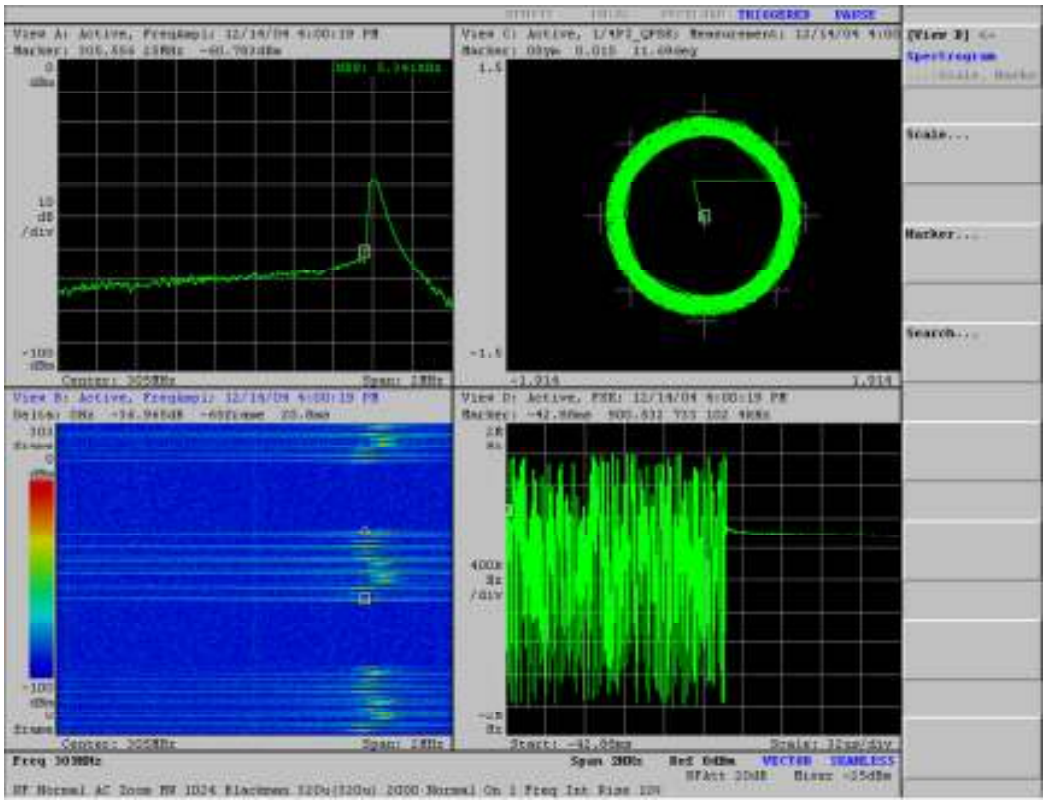


A closer look at the code. Wide and narrow pulses are shown – not really variable length – only two lengths of pulses (dot and dashes) and two lengths of intervals. But the interval length is doubled after every dot. The binary representation of the 29 pulses seems to form the 29-bit command ID (Logic 1 for a dash – logic 0 for a dot, or reversed).

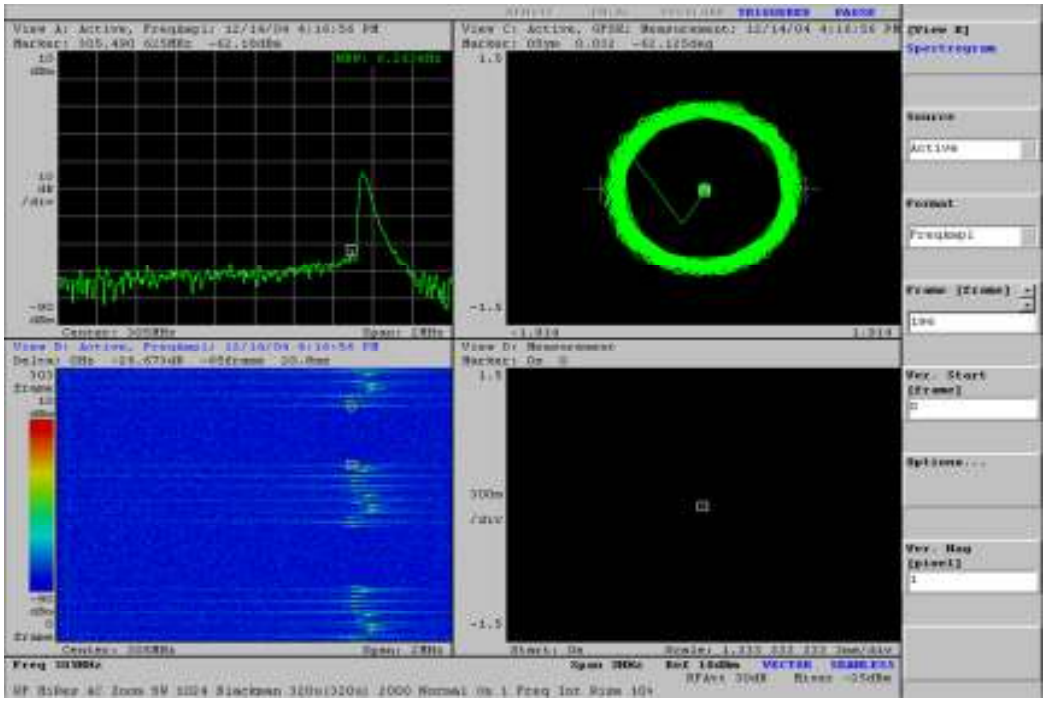
Case 3. German Car Model Mercedes SLK200
Case 4. German Car Model Opel Zafira
Case 5. Korean Car Model Hyundai

Case 6. Taiwanese Garage-Door Opener – General Purpose Remote Control

Case 6. - Cont.

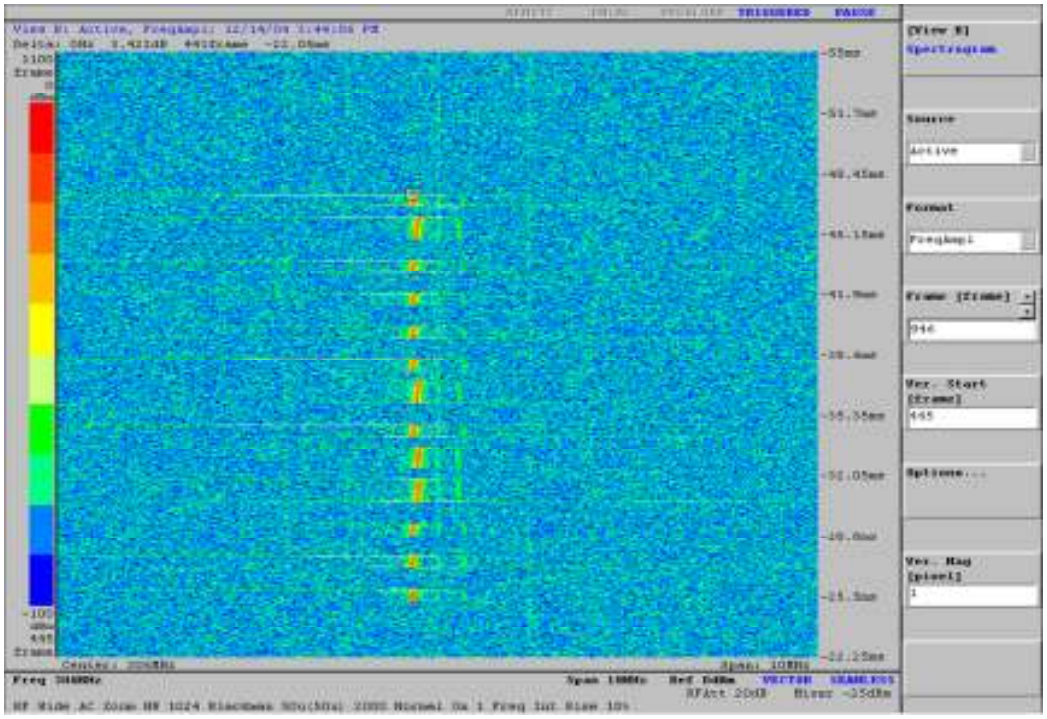


The operating frequency of this device is not stable and drifts from 305.5 to 305.7 MHZ. This is in order to keep costs low. A wideband receiver can handle this easily. The code transmission lasts for about 20.8 msec.



Case 6. - Cont.

Keeping the button pressed, the code repeats every 20.8 msec. This is a kind of FEC (Forward Error Correction) – a simple technique in which, by repeating the code many times increases the probability for the receiver to get it correctly.



A closer look at the code transmission shows dots and dashes again representing digital zeros and ones.

It is found that there is a different proprietary protocol in all cases. Some of the cases utilize code hopping (every time the code is different). The shortest valid command lasts for 13.675 msec minimum from the car-lock types tested (Case 1-Case 5). The car un-locks itself when all of the 13.675 msec transmission is received without errors or jamming. The jammer has to attack for at least a small fraction of that period in order to introduce errors at the receiver that would prevent the car from un-locking. However, there is no any kind of error *correcting* protocol. The error *detecting* protocol available helps the jammer to be very effective because the car simply does not un-locks except only if a valid and correct command is received.

Here are some more examples:

Case 7. Hong-Kong Radio Controlled child-toy
Case 8. Chinese Radio Controlled child-toy
Case 9. Short Range Wireless telephone (headset and base) - not cellular
Case 10. Tri-band GSM/GPRS or other cell-phone
Case 11. Quad-band GSM/GPRS modem
Case 12. Quad-band UMTS (3G) cell-phone
Case 13. DECT Phone
Case 14. Palm-size computer equipped with WLAN or other radio modem
Case 15. Family Radio Service (FRS) or Public Mobile Radio (PMR) license exempt radios, FCC Part 15 devices (US FCC Part 15 of title 47) and model airplane/car/ship/robot remote controls
Case 16. Paging receiver (Pager)
Case 17. Old CB type radio transceiver
Case 18. Baby Monitor
Case 19. Satellite phone
Case 20. Wireless Electronic Doorbell

In order to keep this study short, data for every case or device are not given here. Some cases include “modern” equipment that are very well documented and all of that documentation can be easily found. The most important is that all of the above devices can be easily modified to act as remote controls. All of them are equipped with all of the necessary hardware to assemble an IED remote control in just minutes. Although all of them may not being chosen because of reliability reasons, in this paper are considered as threats.

Especially for Cases 10…14 and perhaps in some kinds of Case 16 there are error-correcting protocols built-in. That means that any jammer preventing only a small fraction of the triggering command of reaching the receiver of an IED is not sufficient and finally a valid command will be extracted at the receiver itself.

Consider for example a GSM cell-phone in an IED. A very simple way of using it is to trigger the detonator from the phone’s ringer. The operator just calls the number of that cell-phone (by using any available means, i.e. his carried cell-phone, a wired phone or by Internet); the phone rings and automatically triggers the detonator. The same can happen using the Short Message Service (SMS). In a more technically advanced application, preventing a false call by chance (someone else to call that number by human or network error) and without the need of waiting for the network

to establish the call or send the SMS, avoiding those delays, the operator may choose to use GPRS (already built-in) and by that way use the phone as a radio-modem. The GPRS connection could be established before the arrival of the convoy. Now, at the appropriate time (when the target is in close proximity to the IED) the operator – observer can send any short data at very high speed (115 kbits/sec), much higher than SMS for example, more that 4 times, in order to trigger the detonator. Using EDGE (see ***Ref. 2***) the GPRS capacity and speed multiplies by three times more! Of course, a kind of an interface is required at the IED phone, but this can be done easily. In the above example, suppose that a jammer is present in the convoy jamming all the GSM frequencies but effectively jams only a fraction of the data traffic. Error-correcting protocols should correct lost data (to a limit) and the detonating command should arrive valid and correct at the detonator, triggering the explosion.

Concluding, there are too many and different threats. Some of them are of higher technology and some of them are "primitive" and really not based on a state of the art in modern communications equipment. If any users of IEDs are ingenious enough, without the need to be technologically advanced, without requiring great resources, money, time and effort they could produce a variety of different kind or type of IEDs and cause serious damages.

Chapter 2

Countermeasures

"A common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools" - Douglas Adams

In the first chapter it has been shown that almost any countermeasures device should have to deal with plenty of different kind of signals and different frequencies. A nearly "perfect" countermeasures system designed to protect convoys may consist of different modules with the following purposes:

1. Early sense the presence of almost all types of explosives.
2. Early sense the presence of almost all types of discharging batteries.
3. Early sense the presence of almost all types of a radio receiver.
4. Early sense and identify the beginning portion of a remote control command. There is only one chance of capturing it; there is no second chance.
5. Engage a jammer powerful enough to protect all of the convoy length and more in order to fully protect the convoy from a late explosion, or from premature explosion if the jammer will actually rig the explosion before the convoy gets close.
6. Alert the crew that there is a threat found and that the jammer has been activated.
7. Record as much of the activity for later review, including any other sensors required. This may help to locate the IED and possibly the capture of the operators.
8. Protect friendly frequencies.
9. Prevent, or cause in purpose, a premature explosion.
10. Should require no any user or at least not a trained user.
11. Should be small enough for mobile mounting in a variety of vehicles.
12. Should be powered from its own battery, which can be charged from the vehicle electrical system or some other external power source.
13. Should be of low cost in order to be installed in as many vehicles as possible.
14. Should be configurable or optionally expandable in order to accommodate for any new types of threats in the future (for example long range Bluetooth or 3G and LTE).
15. Should require minimal maintenance.
16. Should have BITE (Built-In Test Equipment) in order to always ensure its function and alert the crew in the case of failure.

Other options include the semi-permanent installation of a sensor network on the route that a convoy use casually which should alert the convoy vehicles or any other command centers in order to engage a jammer (located at a convoy vehicle or at a sensor) or in order to change plans (i.e. different route). This approach involves installations, testing, maintenance, user training and need for tactics modifications. The use of tactical jammers early moved on the convoy's route before the convoy arrival is another possibility but it involves a great number of resources and personnel.

Tactical planning could be developed in order to aid for the convoy survivability. Cellular base stations can be temporarily shut-off, dummy vehicles appearing as primary targets (not heavily armored decoys) can be employed, very high power air-borne barrage jamming could be used to support the convoy pass from a high-risk area. One other approach is to early drop (from an aircraft) some consumable battery-operated wideband jammers

in all or most of the area that the convoy will pass and thus protect the convoy until their end of life. This also involves a great number of resources and their use in a city area is practically impossible. Image comparison could also help locating IEDs. If detailed optical images of the route are taken and stored earlier and these images are being compared to real time images as the convoy travels then any differences could spot an emplaced device. But this depends on the terrain mostly and if the IED is camouflaged or completely hidden then this approach may not prove to be reliable. However if it would work well, it has the advantage of locating all types of IEDs, not only those controlled be Radio Frequency.

The development of a special counter-IED device looks to be an appropriate solution. Excluding costly or very high volume solutions, a study for a stand-alone, self-contained countermeasures device to constantly accompany the convoy should begin with the decision to use or not to use a kind of an early-warning sensor. This greatly affects system design, cost, size, use, maintenance, convoy-crew morale, opponents' future plans etc.

If an early-warning sensor will not be used, a countermeasures device could be just a kind of a powerful wideband jammer that should be continuously operated. It may jam friendly wireless communications as well and may introduce RFI to many other sensitive devices. In order to keep the power consumption low, a lower power/shorter protection range would be covered and because of the spreading of its power to a very wide range of frequencies, the emitted power density at the specific unknown IED's receiver frequency is not totally ensured that it would prevent the detonation. The existence of any error-correcting protocols would degrade its efficiency further. Continuous operation also raises MTBF (Mean Time Between Failures) and battery capacity issues together with continuous electromagnetic radiation susceptibility of the convoy crew. In addition, the convoy crew would never know if an IED was emplaced somewhere in their route, except of course in the case of a premature or late explosion.

If an early-warning sensor will be used, then a "clever" one has to be developed because of the difficulty of monitoring such a wide frequency range, the variety of threats needed to be identified and the very short time available (some milliseconds) before activating an electronic attack. This sensor would immediately activate a jammer to attack only the frequency spectrum required, only for the time period required. It could be made to protect most of the friendly frequencies and minimize any possible RFI to other sensitive devices at least only for the time period of jamming. A built-in logger together with a GPS receiver could record the event of the jammer engagement and a type of a special search and capture team could collect the IED later, or wait for the IED observer to collect it back and capture him. Power consumption would be much less and the output power available much more effective – the example of ***Fig. 2*** shows a 50dB improvement on the Jammer signal to the IED transmitter's signal ratio (J/S ratio) at the IED receiver. This would prove to be very effective in the case of error correcting protocols or any other kind of IED receiver's "processing gain" available and increases the burn-through range significantly.

It is difficult to calculate the required jamming power because the observer's distance, his transmitter power and frequency and IED exact location are all unknown. Making some assumptions, the following figure is presented (***Fig.2***) and some basic calculations have been done. In the case of a cell phone or pager, the base station location should also be known or estimated.

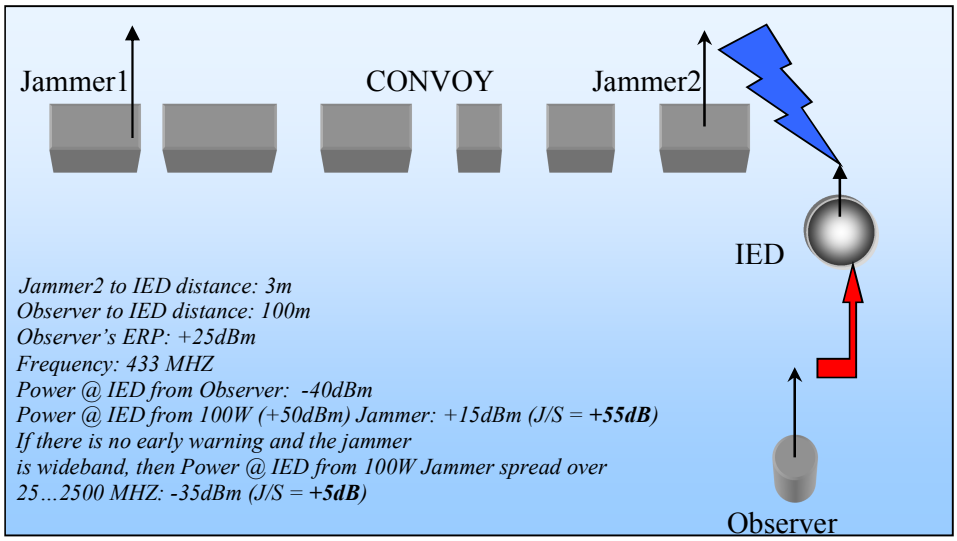


Fig. 2. *The formula used for the propagation Loss (in dB) = -27.6 + 20 log F (in MHZ) + 20 log d (in meters). No any antenna gain has been calculated – all antennae gain involved=0dB. In the case of a cell-phone or pager IED, then the place of the Observer is taken by the nearest base station site.*

In ***Fig. 2***, two (2) jammers are shown. The convoy operator should study this carefully. Another option is one jammer in the middle of the convoy. But if there is a road-turn in a city area with tall buildings and the IED waits after the corner, then the leading vehicles of the convoy may be left unprotected. The reason is that the middle placed jammer will then have some buildings (obstacles) between itself and the leading vehicles, which could degrade its effectiveness (see ***Fig. 3***). By placing one jammer at both ends of a long convoy then there is better coverage. The same applies for any sensor in an early warning device built into the countermeasures system. It is also a function of the convoy length and the wanted front, side and rear protection ranges.

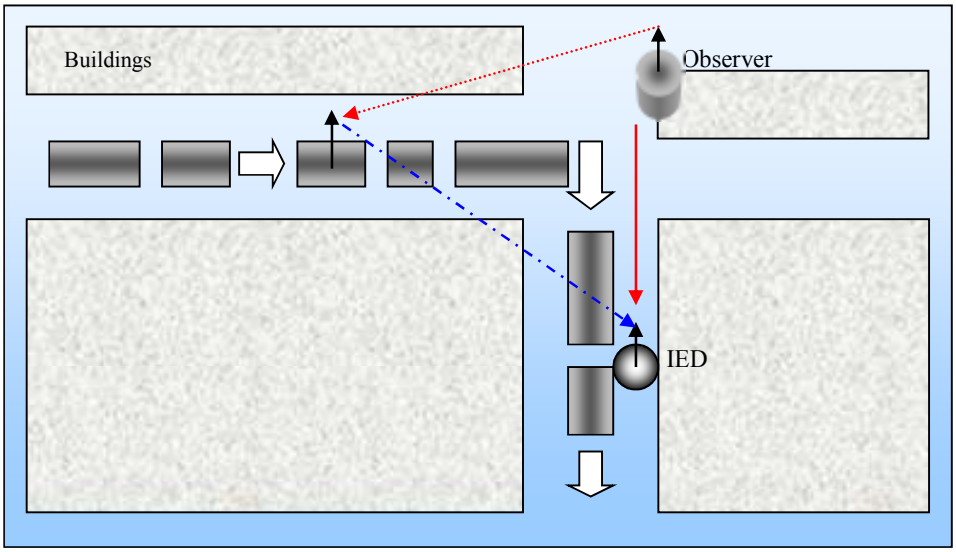


Fig. 3. *A middle placed jammer cannot always protect the convoy.*

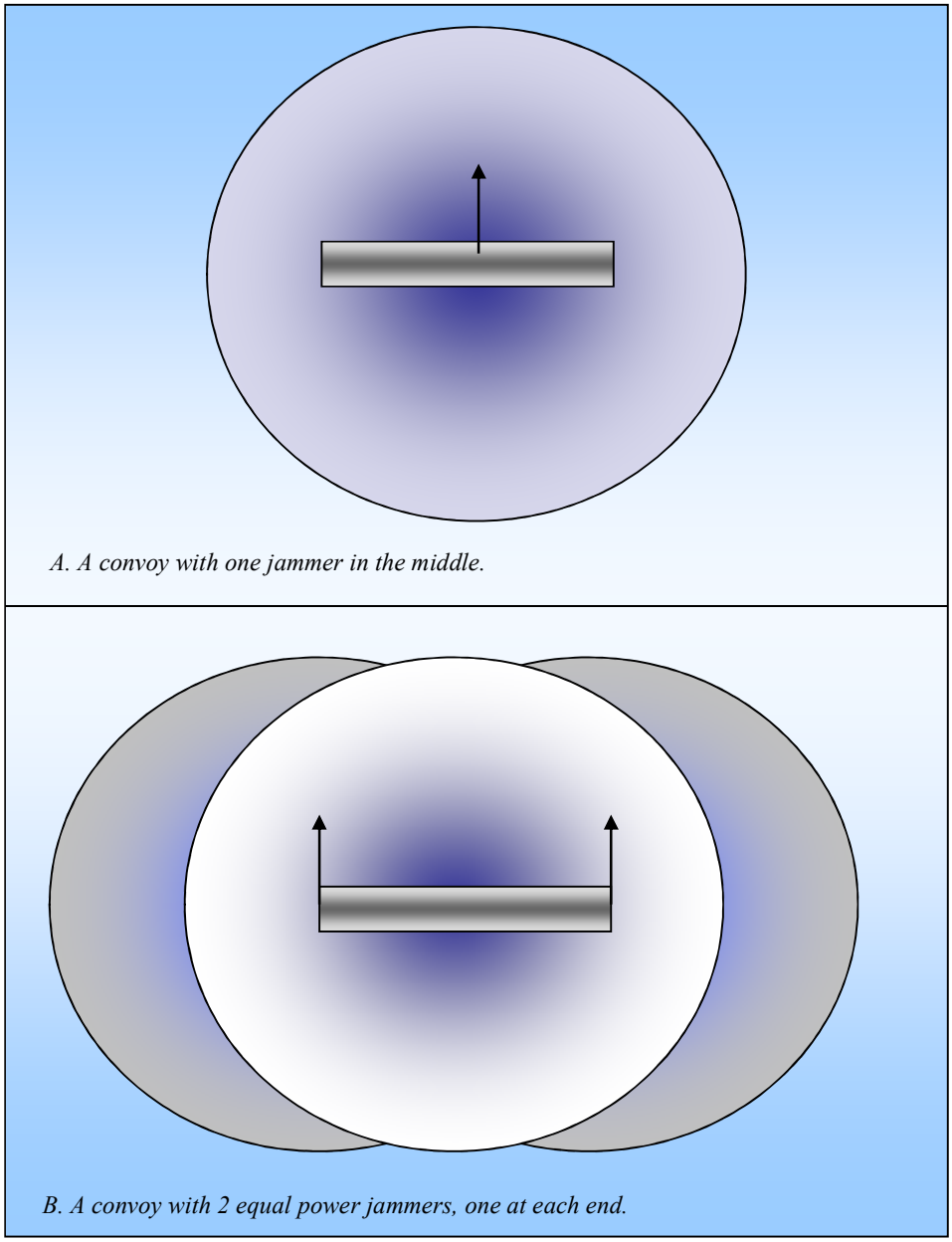


Fig. 4. *The convoy travels from left to right. The blue circles represent the effective range of each jammer. To the right, in front of the convoy, there is an area that is protected or that a jammer can cause a premature explosion. To the left, behind the convoy, there is an area that is protected against a late explosion. At B those area ranges get greater. The middle circle at B is shown as the reference coverage of a middle-placed equal power level jammer.*

In order to establish a given protection range (an ensured jammer effective range with a given burn-through range) then the jammer output power can be calculated with the assumption of observer's transmitter power level. If it is decided that there will be two jammers, then their power levels can be calculated in order to provide the same or greater protection range.

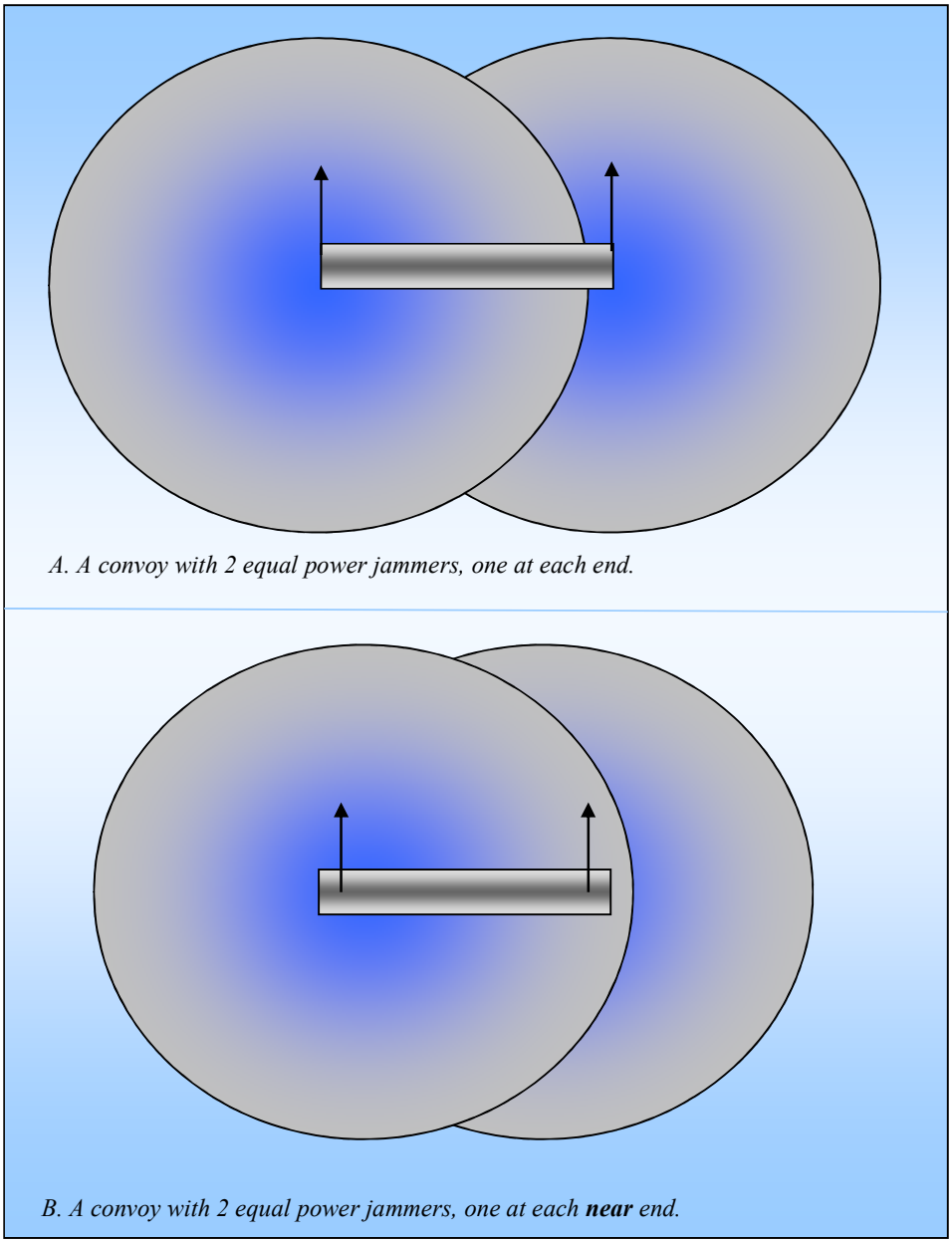


Fig. 5. *The placement of the jammer antennae at each near end reduces the protection ranges at the front and rear of the convoy but increases the protection range at the middle sides.*

In order to help the convoy operator, a single jammer effective protection zone calculating method should be developed, including most of the parameters and then the operator could decide how many jammers he needs for a given convoy length. One idea is to develop special simulation software.

The convoy length and speed of travel affects the minimum time that an electronic attack should last – the hysteresis. A convoy traveling say at 40Km/h, moves 11.1 meters/sec. A 100m-length convoy traveling with this speed is near an IED for about 10 seconds. If 100m in front and 100m at rear protection ranges are added (assuming an IED lethal range of less than 100m)

then this makes a 300m-protection zone moving at 11.1m/sec. So the Jam Duration Time (JDT) must be over about 30 seconds. During this period, the convoy should avoid to stop. Here comes the need for crew notification or alert. In addition, a completely automated logging sub-system can start to collect data from any sensor available (for example shoot some digital photos, save the convoy location coordinates, etc). After that period, the electronic attack will stop and the early warning sensors will operate again. If the same or a new threat is detected then the jamming will be initiated again. Here is one more reason for the early warning sub-system to be quick. If the convoy had stopped because of a well-planned attack to the convoy (the observer had placed obstacles on the road in order to force the vehicles to stop near the IED or he caused a "car accident" ambush) then the electronic attack must continue immediately.

One can expect to have many false alarms during the child age of such a system (a system that has early-warning sensors). Any false alarm (erroneous early detection – not because of an IED presence) will cause an unnecessary jammer engagement. But considering the high value of the human lives or of any other material carried by the convoy then it seems to be not of so much importance, to the point that the friendly communications are not being disturbed constantly. The early detection sensors can be made faster and more intelligent i.e. not just find a threat signal but also try to verify that it as a real threat.

There is a lot of progress to be done on that area. Database matching adds some intelligence here. For example, when a convoy makes a casual route, the countermeasures system can be made to "learn" most of the electromagnetic activity about this route from previous trips on the same route. GPS positioning data can be correlated with the electromagnetic activity data. Inverse database matching would carefully exclude most of the local wireless activity interpreted as threats before, the next time, and effectively identify a new threat.

However, this is very difficult to be applied on GSM like cellular telephony. A semi-complete base station is needed inside the countermeasures system in order to discriminate and identify a real threat between innocent voice conversations but the time before a possible IED explosion is running out in some milliseconds. The cell-phone based IEDs can be treated by "brute force" jamming (sense any activity, then jam all). The consequences of such a decision includes that innocent cellular frequencies will be jammed (near the convoy) for the time period of JDT and the Denial Of Service (DOS) of cell phones.

The early-warning receivers can detect either the frequency of the Local Oscillator (LO) signal radiated from the IED's receiver or the carrier frequency of the observer's transmitter. Fortunately the detection of the LO leakage is possible because of the short distances involved (see ***Fig.7***). Once a signal is detected then the jammer will start to jam at a frequency that corresponds to the detected frequency plus or minus the estimated IF (Intermediate Frequency) of the receiver

of the IED. Another option is, having the LO frequency known, to wait for the transmitter's command signal inspecting a much narrower frequency range and then activate the jammer on the correct frequency. For the first 8 bands (25-465 MHZ), the jammer will transmit all of its available power on the IED's receiver frequency with aim to desensitize the receiver so that it cannot get the command signal from the observer's transmitter. It may also share its power to more than one frequency or spread its power over a defined frequency range. Instead of frequency-sharing its power, time-sharing can be chosen (periodically jam the first frequency, then the next frequency while outputting all of the available power on each frequency). For the rest 3 bands (824-2500 MHZ), where the cell-phones and WiFi operate, any signal activity will engage the jammer to produce a wideband noise signal (band-limited) to cover the bands 7, 8 and 9. This is because, valid criteria for real threat recognition cannot be found. Cost permitted, almost a complete cell-phone base station would be needed inside the VCD in order for the VCD to appear itself as a base station and attack to the cell phones that are located in close proximity. Considering the variety of the cell-phone systems working today around the world attacking the cell-phones can be done by using swept spot jamming and/or noise jamming.

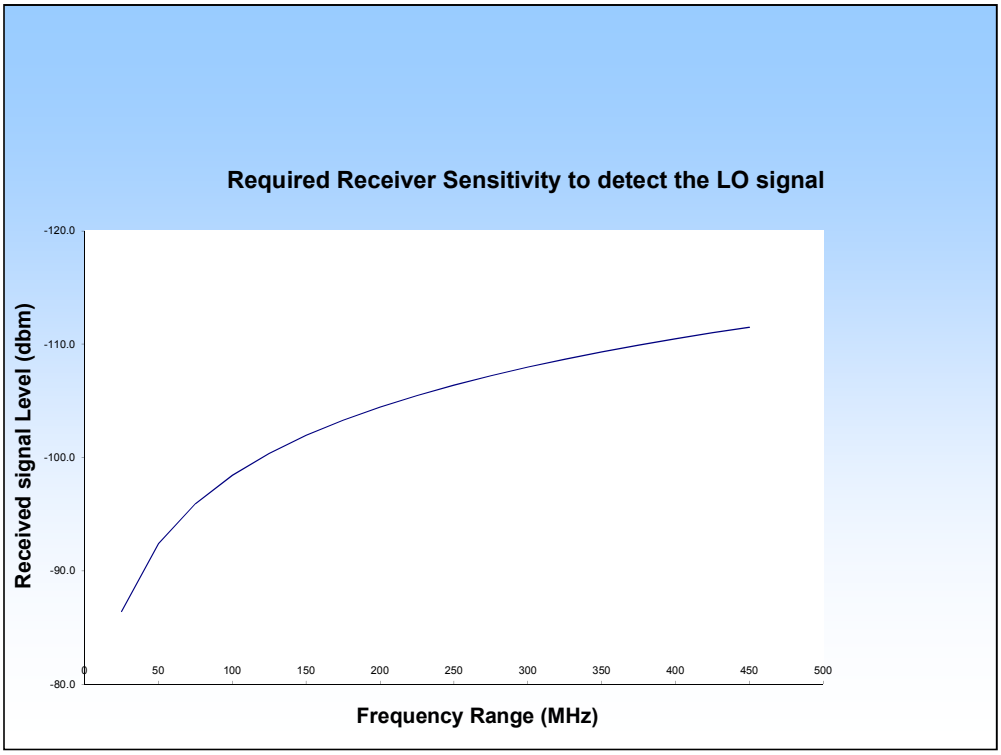


***Fig.** 7 This figure shows the received signal level of a –60 dBm signal level of LO leakage at a distance of 20 meters. The frequency range is from 20 MHz to 450 MHz. It can be seen that the level of the received signal is decreased as the frequency is increased but still the power is enough to be detected be a sensitive receiver.*

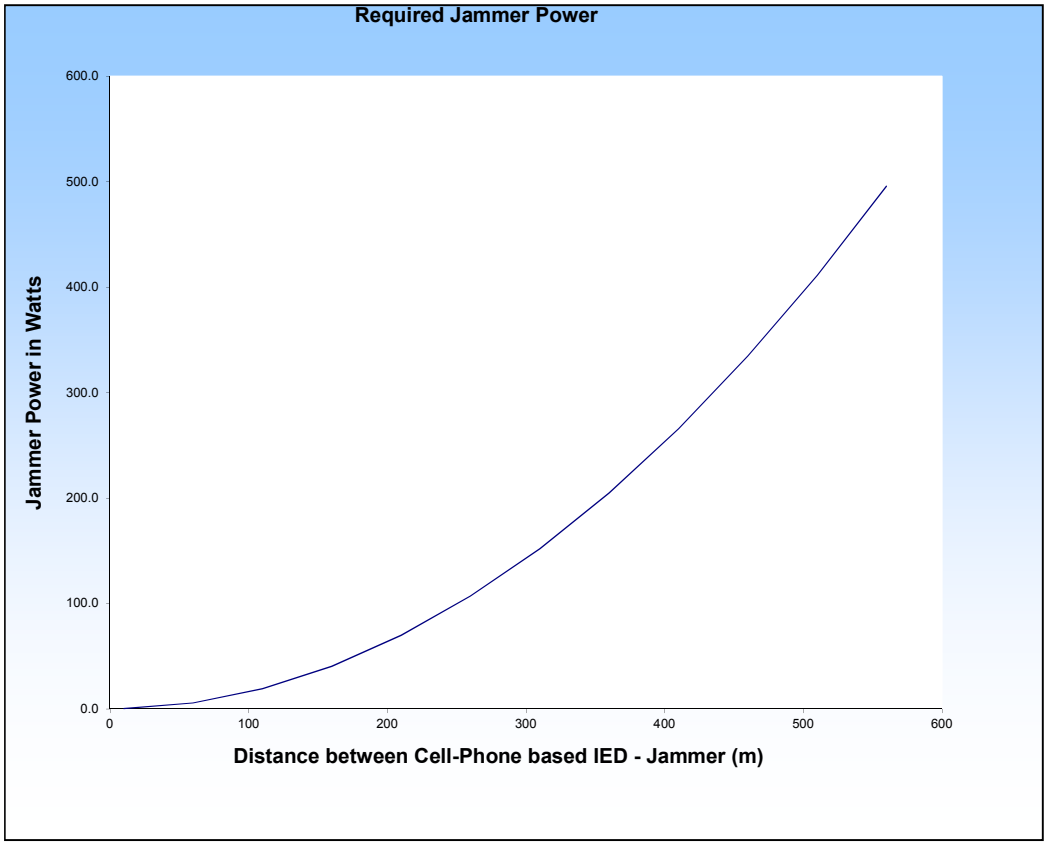


Fig. 8 *This figure is an example, which shows a conservative required power of a jammer (assuming an OMNI directional antenna is used) to jam a mobile phone, which is located 1000 meters away from its base station. As can be seen if the distance between the jammer and the mobile phone is around 100 meters then the required power of the jammer is a few tens of Watts, while, when the distance becomes 600 meters the required power rises to 500 Watts.*

Chapter 4

References

1. *Associated Press - Feb. 26, 2004*

2. *From a cell-phone producer web site (Ericsson).*

Enhanced Data for Global Evolution (EDGE)
A technology that gives GSM the capacity to handle services for the third generation of mobile telephony. EDGE provides three times the data capacity of GPRS. Using EDGE, operators can handle three times more subscribers than GPRS; triple their data rate per subscriber, or add extra capacity to their voice communications. EDGE uses the same TDMA (Time Division Multiple Access) frame structure, logic channel and 200kHz carrier bandwidth as today's GSM networks, which allows existing cell plans to remain intact.

Wideband Code Division Multiple Access (WCDMA)
A technology for wideband digital radio communications of Internet, multimedia, video and other capacity-demanding applications.
WCDMA is the dominating 3G technology, providing higher capacity for voice and data and higher data rates. WCDMA uses a new spectrum with a 5 MHz carrier, providing 50 times higher data rate than in present GSM networks (and 10 times higher data rate than in GPRS networks) WCDMA handles up to 2 Mbps for local area access or 384 Kbps for wide area access. A coming release will include enhancements up to more than 10 Mbps.
WCDMA is also known as UMTS and has been adopted as a standard by the ITU under the name IMT-2000 direct spread. The gradual evolution from today's systems is driven by demand for capacity, which is required by new and faster data based mobile services. WCDMA enables better use of available spectrum and more cost-efficient network solutions. The operator can gradually evolve from GSM to WCDMA, protecting investments by re-using the GSM core network and 2G/2.5G services.

General Packet Radio Service (GPRS)
A packet-linked technology that enables high-speed wireless Internet and other data communications. GPRS provides more than four times greater speed than conventional GSM systems. Using a packet data service, subscribers are always connected and always on line so services will be easy and quick to access.

3. ***Burn-through range:*** *Burn-through occurs when the J/S ratio is reduced to a point where the IED receiver being jammed can adequately get the detonation command from the observer's transmitter. In other words, burn-through range means the effective range of the IED receiver – observer's transmitter link in the presence of the convoy jamming activity. It is the IED receiver distance from its transmitter at which the receiver has adequate signal-to-noise ratio to demodulate and recover the information (detonation command) from the desired signal while being jammed.*

4. *From http://www.infosyncworld.com/news/n/4297.html*

The world first Nokia 5140 lets users push a button to talk over data networks, features a built-in compass, a fitness coach application, integrated camera and much more.

Nokia today unveiled the world's first GSM push-to-talk handset, the sports-inspired Nokia 5140 phone. Along with its ability to connect users at the push of a button, the Nokia 5140 phone also includes a number of unique features designed for active-minded users such as a digital compass, Fitness Coach application and a built-in VGA camera.

The Nokia 5140 is the world's first GSM push-to-talk handset

A GSM/GPRS/EDGE phone, the Nokia 5140 will be available in a GSM 900/1800/1900 MHz version primarily for the Europe/Asia market and in a GSM 850/1900/1800 MHz version primarily for the Americas market. Both versions are expected to be available during the 2nd quarter of 2004.

With the push of a button, Nokia 5140 phone owners can connect to friends and family by using the push-to-talk feature for quick voice communications, or to access the built in VGA camera. The push-to-talk feature can be used to quickly connect the user to one person, or to a group of people by using a key mounted on the side of the handset.

While the Nokia 5140 phone is the first Nokia GSM handset to feature push-to-talk capability, it marks the first step as push-to-talk becomes an increasingly common function. During 2004, Nokia said it will introduce a full range of push-to-talk capable GSM phones, including Symbian OS based smartphones. From 2005 onwards push-to-talk will become available for all Nokia GPRS/WCDMA phones. The "walkie-talkie" style push-to-talk feature of the Nokia 5140 phone is a half-duplex voice over IP (VoIP) solution using the existing GPRS and EDGE data networks that are part of current GSM systems. This method results in performance that according to Nokia is on acerage comparable to that of existing dedicated push-to-talk cellular networks, common in the U.S.

5. *http://www.futaba.com/products/irc/products/telecontrols/index.asp*
6. *http://www.futaba.com/products/irc/products/wireless/index.asp*
7. *www.part-15.org*