

T.G. Benko, I.T. Kohut, V.I. Holota, V.M. Hryha

Computer modeling of mobile devices exposed to radio-electronic interference

Vasyl Stefanyk Carpathian National University, Ivano-Frankivsk, Ukraine, taras.benko@pnu.edu.ua

The paper considers the principle of operation of mobile means of radio-electronic influence. A scheme of a compact device of radio-electronic influence at a frequency of 2.4 GHz is proposed and its modeling is carried out. A method of increasing the power of the device using high-frequency and ultra-high-frequency transistors is proposed. Due to the compact dimensions of the device, it allows it to be integrated as a separate modular element into various electronic interference systems. This device can also be used to suppress the Internet and mobile communications.

Keywords: Radioelectronic impact, mobile device, logic element, frequency controller, signal.

Received 01 April 2025; Accepted 02 December 2025.

Introduction

Modern means of radio-electronic influence are a diverse and complex field. It is constantly evolving, and its effectiveness is systematically increasing. In modern realities, radio-electronic influence is quite important.

First of all, electronic warfare means interfere with the functioning of the enemy's communication and control systems, which makes coordination difficult or impossible, which in turn can lead to chaos in the enemy's information space [1-2]. Thanks to electronic warfare, it is possible to detect and suppress enemy radio, mobile, or satellite communications, disable electronics, satellite navigation, and disorient in space by replacing coordinates with false ones.

The relevance of the study is due to the increasing role of electronic warfare in modern military conflicts. Currently, electronic warfare systems are successfully used to combat unmanned aerial vehicles and communication equipment. They show their effectiveness but require constant improvement and adaptation.

I. Scheme of a compact mobile radio-electronic interference device

Normally our mobile communication works on a certain frequency range. When noise is added in this frequency range, the mobile communication stops working or gets interrupted.

When we add such a frequency range in mobile communication using any scheme, then such scheme is called mobile jammer.

Let's assume that if some applications operate in the 445 MHz frequency range, and we add noise in that range, then these applications will not work properly.

We have developed a circuit for a device for jamming mobile communications in a software environment.

In this circuit, transistor Q1 is in the boost mode and provides the positive feedback needed for generation. The inductor and capacitor are connected to form a tuned oscillator circuit that produces a very high frequency with minimal damping.[3]

Resistor R1 - provides power to the base of the transistor. Resistor R2 - emitter resistor, which helps stabilize the operation of the transistor. Capacitor C3 - separates the DC component of the power supply (5 V)

from the AC, is used for power isolation. And capacitors C4 and C5 - work as filters.

The circuit works like this: 5V power is supplied to the transistor and the LC circuit. Next, the LC circuit forms a resonant frequency, feedback through C1 and C2 feeds part of the signal from the collector back to the base. When the transistor turns on, it amplifies this signal and the process repeats - oscillations occur.

To increase the frequency range, you need to change the values of the inductor (22 nH) and capacitor (15 pF). As the values of these two components decrease, the range will increase.

To determine what frequency range the circuit will produce, you need to use the formula:

$$\frac{1}{2 \times \pi \sqrt{L \times C}}$$

The oscillation frequency for this circuit is 131.83 MHz.

If we take a capacitor with a capacity of 1 pF and a coil with an inductance of less than 22 nH, then the circuit will produce a frequency of 1 GHz, that is, the circuit will be able to jam frequencies up to 1 GHz.

Figure 3 shows a graph of frequency versus capacitance and frequency versus inductance. Accordingly, the left graph shows that the greater the inductance, the lower the frequency. And this is logical, because the resonant purity is inversely proportional to \sqrt{L} . The right graph shows that the greater the capacitance, the lower the frequency. Therefore, by reducing L and C, the frequency of the generator can be increased.

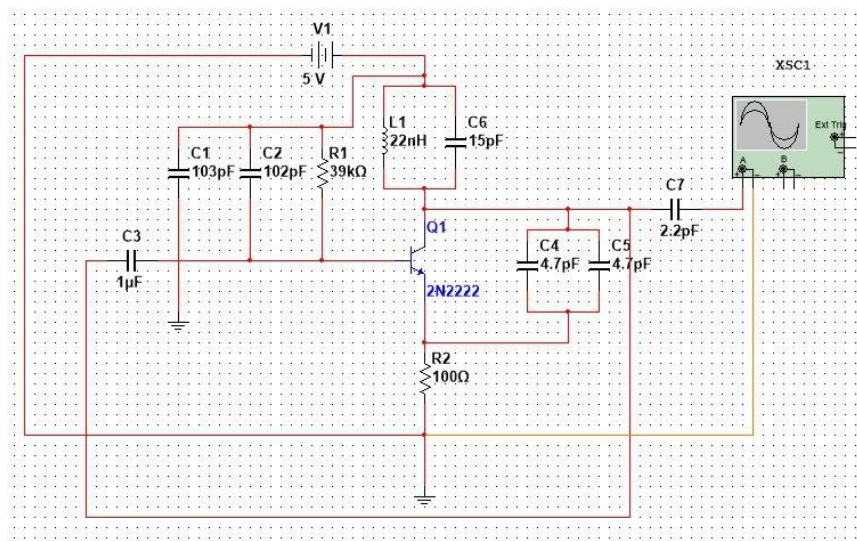


Fig. 1. Schematic diagram of a mobile phone jamming device.

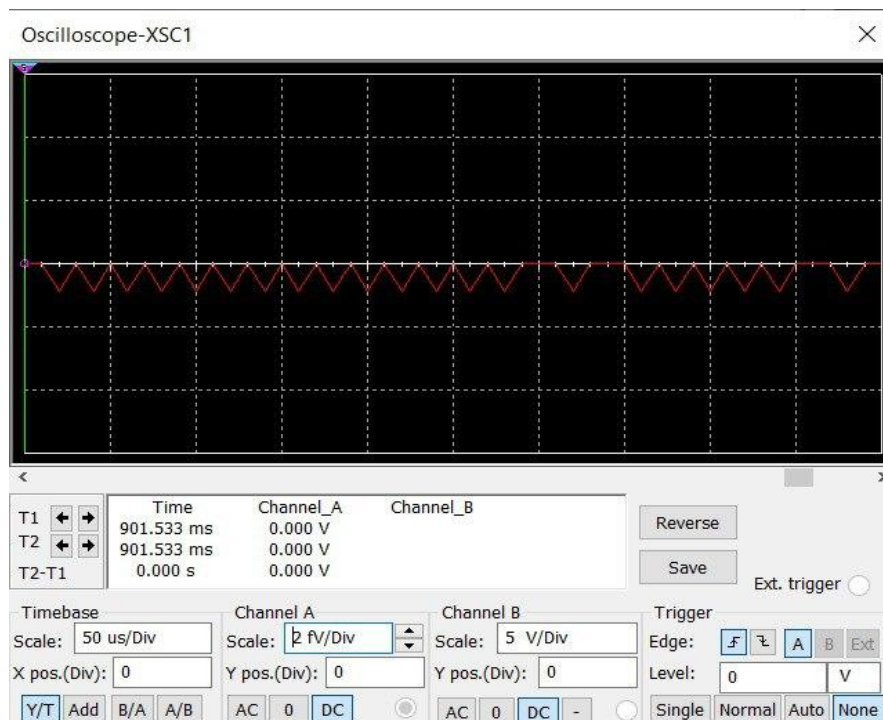


Fig. 2. Frequency with minimum damping.

II. Mobile device for radio electronic interference at a frequency of 2.4 GHz

Figure 4 shows a circuit where two identical generators are placed, each on a pair of parallel KT610 transistors. The generator is built using the Miller effect, so it will not work on a single transistor [4]. The generation is unstable, which leads to a very wide generation spectrum, from hundreds of kilohertz to almost the upper frequency limit of the transistors used.

It shows a power of about 1 watt to silence televisions and internet connections. Parallel connection of two or more transistors allows to significantly increase the total power, but some measures are required to evenly distribute the current across each, for example, "leveling" resistors in the emitters with a nominal value of 0.1 to 10 Ohms, depending on the transistors [5].

It is quite possible to increase the power of the device to several tens of watts. The type of transistor affects both the output power and the type of spectrum of the generated signals. You can use almost any high-frequency and ultra-high-frequency transistors, based on the total power and limiting frequency of the devices used, and the important

types of supply voltages for which the transistors used are designed. In no case should you exceed the maximum current of the transistor, otherwise it will burn out. It is better to limit it with a powerful resistor to a value of 0.7...0.8 of the maximum allowable. Let's say the maximum collector current according to the manual is 2A, the typical supply voltage is 12V. We use 4 transistors. We get the maximum permissible current per transistor of 1.4 A. 4 transistors - therefore, the total current of the device should not exceed 5.6A. This is the limit value at which very good, preferably forced, cooling of the transistors is required.

Figure 5 shows the assembled circuit in Multisim. Where +12 V is supplied, the circuit starts operating as a high-frequency generator.

The first two transistors form a switching cascade that operates in high-frequency mode. The next two transistors do the same. And the inductance together with the transistors form the generation of a 2.4 GHz signal, which overlaps the operating range of Wi-Fi.

So, this is already a fairly powerful RF generator that creates broadband interference in this range, blocking communication over a fairly large radius.

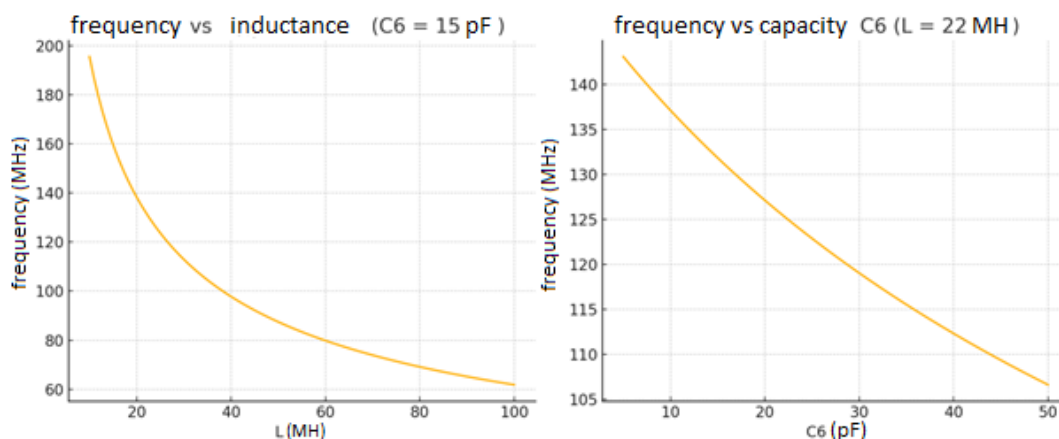


Fig. 3. Dependency graph of frequency versus capacitance and frequency versus inductance.

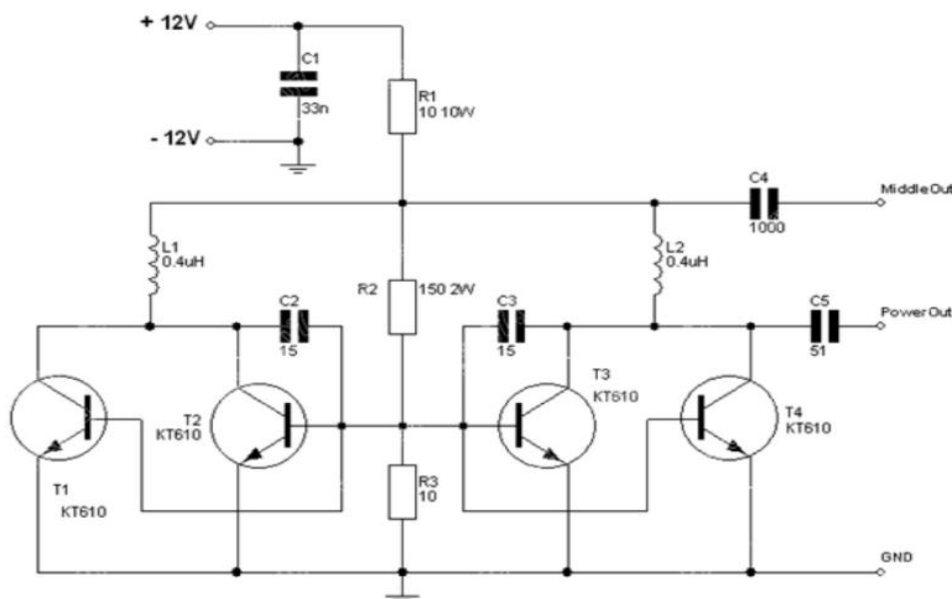


Fig. 4. GHz jamming device diagram.

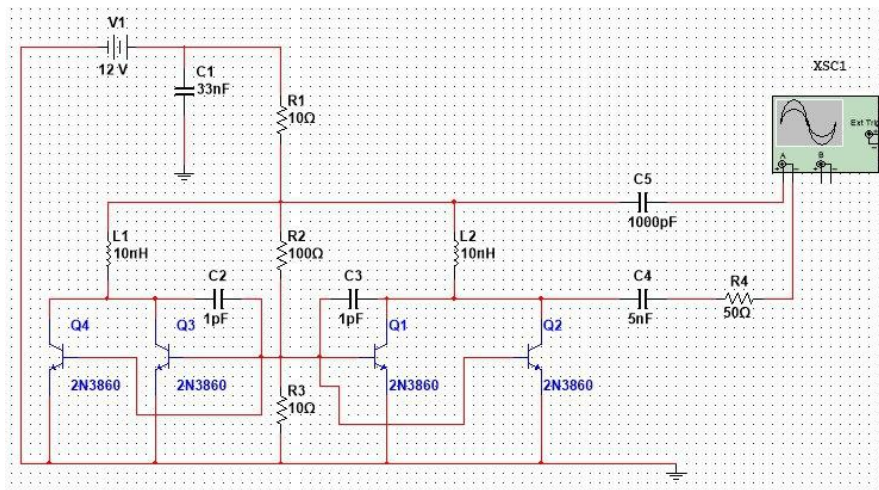


Fig. 5. GHz jamming scheme.

III. Development prospects

Mobile electronic warfare assets are most effective when integrated into an overall intelligence, command, communications, and attack system. Their operation in the context of combined operations (ground forces, aviation, drones) enhances combat power. This concept usually refers to portable or platform (vehicle) vehicles and devices that can create electronic interference, detect radio signals, or perform electronic reconnaissance in mobile conditions. Mobility allows you to quickly deploy electronic warfare closer to your targets, change positions, and avoid being hit. Mini modules - tactical mission boards - modular solutions that can be integrated into other platforms (intelligence, anti-drone systems, etc.) [6].

Mobile electronic warfare devices are becoming one of the decisive factors in ensuring information superiority on the battlefield. Thanks to their flexibility of deployment, rapid change of positions, and adaptability, they are able to significantly influence the effectiveness of the enemy's actions.

On the one hand, mobile electronic warfare can suppress communications, navigation, and control, significantly limiting the enemy's combat capabilities. On the other hand, one's own platforms and communications need protection from similar enemy actions. Success depends on a well-thought-out balance between offense and defense.

The autonomy of mobile systems depends on power sources, range, and quality of antenna systems. In addition, the risks of collateral effects (on civilian networks, other electronic systems) must be taken into account when deploying in densely populated areas [7].

Conclusions

The radio electronic interference scheme we developed has shown its high efficiency in suppressing the Internet and mobile communications at a frequency of 2.4 GHz. And its compactness makes it possible to integrate it into various mobile radio electronic interference devices.

To ensure effective protection, large resources are required: significant power, large installations and separate modules for each of the antennas. This complicates mobility and requires serious technical support.

At the same time, it is impossible to abandon the development of electronic warfare - it is a key element of information and technological confrontation. Therefore, despite all the difficulties, it is necessary to continue to improve approaches, adapt strategies and develop more effective means of counteraction in the conditions of the constantly changing nature of hostilities.

Benko T.G. – Doctor PHD, Assistant Professor, Department of Computer Engineering and Electronics.

Kohut I.T. – Doctor of Technical Sciences, Professor of the Department of Computer Engineering and Electronics;

Holota V.I. – Candidate of technical sciences, associate professor, associate professor of the department of computer engineering and electronics;

Hryha V.M. – Candidate of technical sciences, associate professor, associate professor of the Department of Computer Engineering and Electronics.

- [1] O.M. Chernysh, G.V. Pevtsov, S.V. Pshenichnykh, A.Ya. Yatsunenkov, *Prospects for the development of electronic warfare taking into account the experience of NATO countries*, 36th scientific works of the Joint Research Institute of the Armed Forces, 1(1), 15 (2005); http://nbuv.gov.ua/UJRN/Nitps_2010_1_31.
- [2] S.O. Tyshchuk, S.M. Sholokhov, *Electromagnetic weapons as the basis for the formation of a new ideology of electronic warfare in modern armed struggle and in the future*, Super-Volonter, 5(37), 18 (2005).
- [3] V. G. Sholudko, V. V. Olshansky, S. A. Pyvovarchuk, M. I. Stoychev, V. V. Filipov, *Organization of military communications* (Geroiv Krut Military Institute of Telecommunications and Informatization, Kyiv, 2023).

- [4] O. M. Chernysh, G. V. Pevtsov, V. I. Volkov, V. A. Lupandin, S. V. Zakirov, G. V. Megelbei, *Information and calculation system of the heads of electronic warfare services of military command bodies*, Science and Technology of the Air Force of the Armed Forces of Ukraine, 2(2), 71 (2009).
- [5] I. K. Nesterenko, O. P. Fedienko, *Low-visibility radio stations of the soldier*, Wireless Ukraine, 22, 3-8 (2018); 23, 11-17 (2018).
- [6] S.M. Sholokhov, E.V. Luchuk, O.B. Zavatsky, *Trends and promising directions of development of electronic warfare*, Arsenal-XXI, 12(38), 39 (2006).
- [7] G.V. Pevtsov, S.M. Sholokhov, G.M. Tikhonov, I.M. Tikhonov. *Scientific foundations of substantiation of methods of combat use of forces and means of electronic suppression in operations*, Control, navigation and communication systems, 3(7), 120 (2008).
- [8] S.M. Sholokhov, Yu.V. Gordienko, *Methodology for developing scenarios for radio electronic and electromagnetic suppression of the national telecommunications network and complex signal-interference environment for the synthesis of adaptive interference protection algorithms*, Proceedings of the Academy, 17(167), 127 (2020).

Т.Г. Бенько, І.Т. Когут, В.І. Голота, В.М. Грига

Комп'ютерне моделювання мобільних пристроїв радіоелектронного впливу

Карпатський національний університет імені Василя Стефаника, м. Івано-Франківськ, Україна, taras.benko@pnu.edu.ua

В роботі розглянуто принцип роботи мобільних засобів радіоелектронного впливу. Запропоновано схему компактного пристрою радіоелектронного впливу на частоті 2,4 ГГц та проведено її моделювання. Запропоновано спосіб підняття потужності пристрою за допомогою високочастотних та надвисокочастотних транзисторів. Завдяки компактності габаритних розмірів пристрою, дає змогу інтегрувати його як окремий модульний елемент у різноманітні системи радіоелектронного впливу. Також даний пристрій може використовуватися для подавлення інтернету та мобільного зв'язку.

Ключові слова: Радіоелектронний вплив, мобільний пристрій, контролер частоти, сигнал.