ACTIVE JAMMER STATIONS

Grigorik I.A., gr. 050503

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Kupriyanova D.V. – MS of technical sciences.

This paper provides an overview of the key characteristics, features, and design nuances of active jamming systems, including active jammer stations. It also briefly examines the legal restrictions applicable to similar devices within the Republic of Belarus.

An active jamming station is a signal-blocking device that transmits (usually random) signals on the same frequency at which the target signal needs to be blocked. Most often, frequency-based design accounts only for the frequency that must be blocked. However, the polling frequency of the receivers of the devices operating at that frequency should also be taken into account. For example, in Bluetooth devices the polling frequency is at least 125 Hz, i.e. one poll every 0.008 seconds [1].

The minimum response frequency to a packet must also be taken into account. Taking Bluetooth as an example again, the *802.15.1* standard specifies a minimum response time of 625 microseconds, i.e. a frequency of 1600 Hz [2], from which it follows that these devices can operate at a maximum rate of 1600 minimally-filled packets per second. Accordingly, frequency-based design must ensure that at least one noise pulse is generated at the minimum response frequency, in an attempt to block a message that may be received at that same moment on the given frequency. This can be achieved, for example, by exhaustively sweeping the spectrum, which can be represented as the graph shown in Figure 1.

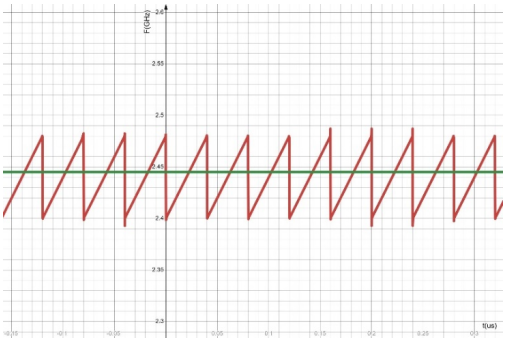

Figure 1: Example graph of the useful signal and noise over time

In this graph, the red line represents the frequency-versus-time relationship, while the green line represents the linear frequency-versus-time relationship of the information signal. For simplicity, this example does not take FHSS modulation into account, nor the fact that channels can change over time. According to this graph, the jamming signal sweeps through the frequency range in which data transmission occurs. Moreover, several noise messages may be generated during the transmission of a single packet, since this in no way hinders the blocking of the signal.

The next thing to take into account is the operating frequencies. If the task is to generate noise at the Bluetooth or Wi-Fi 2.4 GHz frequency, it is necessary to operate at frequencies from 2400 to 2483.5 MHz, for which, for example, voltage-controlled oscillators (VCOs) can be used. These devices allow a signal of a given frequency to be generated, set by the level of the input voltage. Moreover, a single device may contain several VCOs operating at different frequencies, providing greater coverage of the frequencies to be blocked. The advantage of using VCOs is that, when blocking a signal by sweeping, there is no need to build a device that operates at ultra-high frequencies – it is enough to generate the same sawtooth pulse, except that instead of a frequency, a voltage must be set at which the VCO itself will generate the ultra-high-frequency signal. For example, taking the YSGM232508 module, whose input-voltage-to-output-frequency relationship is shown in Figure 2, a device can be built that generates sawtooth pulses at a frequency of 2000 Hz, at a voltage of 3.5 to 4.5 V, which allows the entire Bluetooth frequency spectrum to be swept at that rate.

It is important to understand that active jamming stations do not attenuate signals present over the air. The generated interference likewise travels over the air and is picked up by receivers. As a result, information signals are drowned out

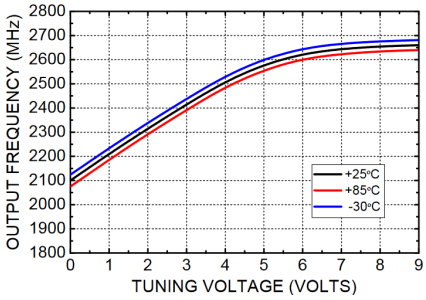

Figure 2: Output frequency versus input voltage of the YSGM232508 module [3]

and are not processed by the receiver. To determine whether a signal will be blocked, the signal-to-noise ratio (SNR) is used, which can be expressed by several formulas. If the signal is measured in decibels, the ratio is obtained simply by subtracting the noise from the useful signal, as expressed by Equation (1):

$$SNR = S - N \tag{1}$$

where S is the signal quality (dB), N is the amount of noise (dB), and SNR is the signal-to-noise ratio (dB).

However, if the signal is measured in watts or volts, the ratio of the quality signal to the noise power must be formed, taking the logarithm and multiplying it by an additional coefficient (see Equation (2)).

$$SNR = M \cdot \lg(S/N) \tag{2}$$

where M equals 10 if measured in volts, or 20 if measured in watts.

For this SNR formula, a scale is used whereby a signal of 5 to 10 dB is considered indistinguishable due to the high level of noise, 10-15 dB is the minimum for establishing an unreliable connection, 15-25 dB is a poor connection, and 25-40 dB is a good connection. Anything above that is considered an excellent connection [4]. Accordingly, to block a signal, noise must be generated at a higher power, which is one of the key characteristics of jamming stations - the transmitter's output power.

However, within the territory of the Republic of Belarus there are certain restrictions related to the maximum transmitter power of devices. According to part one of Article 28 of the Law of the Republic of Belarus, the right to use the radio frequency spectrum is granted through the allocation of radio frequency bands, radio frequency channels, or radio frequencies, and/or the assignment of a radio frequency or radio frequency channel. At the same time, according to the Belarusian State Inspectorate for Telecommunications, there are cases in which obtaining permits for the operation of wireless broadband radio-electronic equipment is not required – for example, devices operating at frequencies of 2.4 GHz with a radiated power of no more than 100 mW [5].

Active jamming stations are widespread and important today both in the field of specialized military equipment and in civilian equipment. In military equipment, these stations are designed to counter guided missiles, UAVs (unmanned aerial vehicles), and radio communication stations. In the case of civilian equipment, they are commonly used to counter terrorism, protect privacy, and prevent cheating (e.g., during exams).

References

[1] What is the difference between bluetooth and 2.4 ghz? https://www.meetion.com/what-is-the-difference-between-bluetooth-and-24-ghz, 2023. Accessed: 2024-04-03.

[2] IEEE. Part 15.1: Wireless medium access control (mac) and physical layer (phy) specifications for wireless personal area networks (wpans). Technical Report IEEE Std 802.15.1, IEEE, New York, 2005.

[3] Ysgm232508 datasheet. https://www.lcsc.com/datasheet/C52043361.pdf, 2024. Accessed: 2024-04-03.

[4] What is signal to noise ratio and how to calculate it? https://resources.pcb.cadence.com/blog/2020-what-is-signal-to-noise-ratio-and-how-to-calculate-it, 2020. Accessed: 2024-04-03.

[5] Frequently Asked Questions. https://www.belgie.by/ru/faqs/, 2024. Accessed: 2024-04-03.