UDK: 355.43:623.624,449.8
COSATI: 03-10, 14-04-01
doi: 10.5973/str2102046R

Sweep Jamming with Discrete Subbands – an Advanced Strategy for Malicious Drones Missions Prevention

Jovan Radivojević [1)]
Branislav Pavić [1)]
Aleksandar Lebl [1)]
Milena Petrović [2)]

Malicious drones jamming is a subject of numerous researches in the world. The implemented jamming strategy is different in various cases and each improvement in the analysis, modeling and realization contributes to the jamming procedures originality. In this paper, we have analyzed implementation performances of sweep jamming with discrete subbands. This advanced method allows decreasing the problems caused by drone communication and/or telemetry signals jamming on the undesired disruption of navigation signals (GPS and GLONASS) used for the localization of friendly devices in the drone vicinity. The problem is analyzed on the example of one signal frequency intended for drone communication with its operator. Drones with this specific signal frequency are used relatively rarely, but the obtained results are the most illustrative for practical consideration of the problem. The specificity of this frequency is that it is nearest to the navigation signal frequencies which means that important conclusions made for this frequency are satisfied significantly easier for other frequencies intended for drone communication, video and telemetry signals transmission.

Key words: **malicious drones, sweep jamming, discrete subbands, communication and telemetry signals, navigation signals.**

Introduction

NOWADAYS the usage of drones (or unmanned aerial vehicles – UAVs) becomes more and more convenient. The new drone implementation areas constantly appear, and the number of operable drones increases every day. However, in parallel to the drones (or unmanned aerial vehicles – UAVs) increased usage in friendly operations, drones are more and more applied in malicious missions. It is often not easy to predict such malicious missions, meaning that the final consequences of these missions are great material losses and/or human victims [1, 2]. References [1] and [2] just present one example when coordinated drones attack have produced a great damage while [3] and [4] give a comprehensive survey of possibilities to implement drones for malicious purposes. There is a high number of solutions for malicious counter drone technique implementation and [5-10] compose only a small survey of examples. Some other solutions, which are applied in the world, are briefly presented in [11].

Usually applied techniques for drone jamming are the same as for other system types jamming: for remote controlled improvised explosive devices (RCIEDs) activation prevention [12-14], for RF (HF and VHF/UHF) spectrum jamming [15-16] and for mobile systems communications jamming [17]. These techniques are barrage, tone and sweep jamming. In some cases, malicious drones operation is jammed using pulsed RF signal that is additionally swept [18]. Besides, protocol-aware jamming is also suitable for malicious drones jamming [19, 20]. Sometimes the aim is not to cause drone operation jamming, but to realize spoofing, i.e. to take over the control of drone flight and function [21]. The effectivenes of applied drone signals jamming techniques is estimated on the base of Bit Error Rate (BER) determined by calculation or simulation [22].

The most effective way to disable drone operation is to jam its navigation system (GPS and GLONASS) and all already applied jammer solutions have the possibility to disrupt these signals [18, 5-10]. The other signals used in drone operation are not always jammed or only some of them are jammed. Nearly all possible signal frequencies are jammed in [23]. Our aim has also been to jam all the systems used for drone operation and to consider the applied frequencies for these functions in various drone types in order to increase reliability of successful jamming [24, 25]. In our solution, we have implemented a strategy sweep jamming with discrete subbands that is rarely found in existing jammers. According to our knowledge, this jamming strategy has not been applied in other similar systems for malicious drone jamming. Sweep jamming with discrete subbands has been implemented in systems for RCIED activation prevention.

Characteristics of signals used for drone operation are presented in the Section 2. Multisweep jamming with discrete subbands is analyzed in the Section 3 and its characteristics are compared to multisweep jamming with continual subbands and to pure sweep jamming. Performances (first of all frequency characteristic) of the generated multisweep signal with discrete subbands and its influence on the navigation signal reception in hostile and friendly receivers are investigated in the Section 4. The possibility to adapt the

[1)] Department for Radiocommunications, IRITEL a.d., Batajnički put 23, 11080 Belgrade, SERBIA
[2)] Military Technical Institute (VTI), Ratka Resanovića 1, 11132 Belgrade, SERBIA
Correspondence to: Aleksandar Lebl , e-mail: lebl@iritel.com

analyzed algorithm for jamming modern drone communication scenarios is described in the Section 5. The paper conclusion is in the Section 6.

Characteristics of signals used for drone functioning

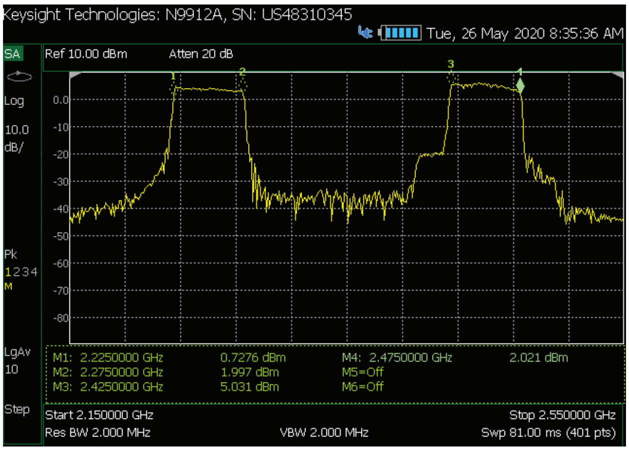
There are three groups of signals used for a drone functioning: 1) communication signals between the drone and its operator; 2) video and telemetry signals that are sent from drone to its operator; 3) satellite navigation signals (GPS or GLONASS) used for drone flight control. Among all these signals, telemetry signals may include data about drone battery status, drone speed, altitude and direction of flight, air temperature and drone launch location, etc [26]. Telemetry data is collected using various drone sensors such as accelerometer, gyroscope, infrared and temperature sensors, RF receivers, cameras, and so on. The three groups of signals differ one from the other in the applied signal frequencies, signal power levels and the applied channels width, meaning that they differ in the necessary total energy per channel. The frequencies applied for drone communications and for video and telemetry links are 433 MHz, 868 MHz, 915 MHz, 1.2 GHz, 1.3 GHz, 2.4 GHz, 4 GHz, 5.8 GHz, 8GHz, while 1176 MHz, 1227 MHz and 1.57-1.62 GHz are used for locating by GPS or GLONASS systems [27-29, 18]. Although located in the same group 2) of signals according to the direction of signals transmission, drone video and telemetry signals use different signal bands (frequencies). Nowadays the most popular frequency band for video signals transmission is 8GHz and frequencies about 400 MHz and 900 MHz are most often applied for telemetry signals transmission [29]. The older drone systems use frequencies 27 MHz, 35 MHz, 49 MHz, 72 MHz or 75 MHz [30]. Nowadays about 90% of drone types use frequencies 2.4 GHz and 5.8 GHz for communication and downlink video signal transmission [31]. The power levels of the first two signal groups (communication, video and telemetry signals) are significantly higher than the power levels of the third group: the power levels of satellite navigation signals at the place of their reception may be in the range depending on the time interval in the process of localization and conditions of such localization [32]. It is important to notice the fact that the set of applied frequencies for drone operation is a priori known (standardized), opposite to signal frequencies applied for RCIED activation.

$$n_0 = -130\ dBm \quad \text{to} \quad n_1 = -160 dBm \qquad (1)$$

If we now consider all applied signal frequencies and signal amplitude levels, three important conclusions may be made. The first one: frequencies intended for communication, video and telemetry signals are mutually mixed with GPS and GLONASS signal frequencies. The second one: frequency gap between the signals for communication, video and telemetry on one side and navigation signals on the other side is variable. The narrowest gap is between communication and downlink video signal frequency operating at 1200 MHz and two nearest navigation signal frequencies operating at 1176 MHz and 1227 MHz. The third one: too high jamming signal power level at the frequencies of navigation signal would mean that navigation would be disrupt in a wide area around the jammer, perhaps significantly wider than it is necessary to disable the malicious drone operation. In this way, many friendly devices and systems around the jammer are also unnecessarily disrupted.

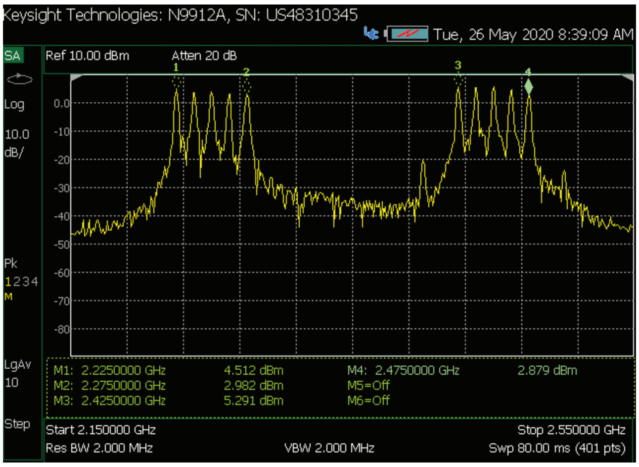
Multisweep jamming with discrete subbands

Sweep signal generation is the well known strategy of jamming. The generated signal frequency is variable with time. Linear change of signal frequency is the most often applied.



```
Keysight Technologies: N9912A, SN: US48310345
                                        Tue, 26 May 2020 8:35:36 AM
SA    Ref 10.00 dBm        Atten 20 dB
Log
10.0
dB/
Pk
1234
M
LgAv   M1:  2.2250000 GHz      0.7276 dBm     M4:  2.4750000 GHz      2.021 dBm
10     M2:  2.2750000 GHz      1.997 dBm      M5=Off
       M3:  2.4250000 GHz      5.031 dBm      M6=Off
Step   Start 2.150000 GHz                                        Stop 2.550000 GHz
       Res BW 2.000 MHz              VBW 2.000 MHz        Swp 81.00 ms (401 pts)
```

Figure 1. Frequency characteristic of continual multisweep signal



```
Keysight Technologies: N9912A, SN: US48310345
                                        Tue, 26 May 2020 8:39:09 AM
SA    Ref 10.00 dBm        Atten 20 dB
Log
10.0
dB/
Pk
1234
M
LgAv   M1:  2.2250000 GHz      4.512 dBm      M4:  2.4750000 GHz      2.879 dBm
10     M2:  2.2750000 GHz      2.982 dBm      M5=Off
       M3:  2.4250000 GHz      5.291 dBm      M6=Off
Step   Start 2.150000 GHz                                        Stop 2.550000 GHz
       Res BW 2.000 MHz              VBW 2.000 MHz        Swp 80.00 ms (401 pts)
```

Figure 2. Frequency characteristic of multisweep signal with discrete subbands

The frequency characteristic of continual multisweep signal is presented in Fig.1. The example characteristic was measured in the process of drone jammer initial testing and verification [24, 25]. The jamming signal consists of two continual subbands thus forming a multisweep signal. The signal amplitude level in the subband is generated as constantly equal in the whole frequency range. The bandwidth of each of these two subbands is 50 MHz. The first one covers frequency range 2225–2275 MHz and the second one covers 2425–2475 MHz. Resolution bandwidth (frequency step) to record and display the presented frequency characteristic is 2 MHz and sweep time is 80 ms.

The frequency characteristic of multisweep signal with discrete subbands, which is the subject of this paper analysis, is presented in Fig.2. In the practical realization jamming on each discrete frequency within the continual subband is realized on a single frequency (as a tone or spot jamming). The time used for jamming on this single frequency is in this case longer than when sweep jamming is applied, thus increasing jamming reliability for this frequency. Throuhout this paper tone jamming is replaced by sweep jamming where the swept frequency range is considered to be very narrow. Besides, the sweep rate is supposed to be equal as if the whole continual subband is swept. It means now that sweep jamming in discrete subbands is analytical model for practically realized tone jamming. The swept frequency range in a discrete subband j (Δf_j) may be now calculated as:

$$\Delta f_j = f_{\max j} - f_{\min j} = \alpha \cdot T_j \tag{2}$$

where α is the sweep signal rate and T_j is the time of tone jamming on a single frequency.

According to this, the parameters for the graph in Fig. 2 (bandwidths, resolution bandwidth, sweep time) are the same as in Fig.1 with the exception that there are 5 frequency characteristic peaks at mutual distances of 12.5 MHz in the frequency bands 2225–2275 MHz and 2425–2475 MHz instead of equal signal power level in these two frequency bands. The power level of signals in each subband is equal in the presented case, but there is a possibility in the realized drone jammer to define different signal power level for each subband. The discrete subbands of the jamming signal in Fig.2 have equal bandwidth, but there is a possibility to generate signals in different frequency bandwidth for different subbands. The a priori known frequencies applied for drone functioning allow us to apply sweep jamming with discrete subbands.

The contribution of multisweep jamming with continual frequency subbands comparing to pure sweep jamming and, further, multisweep jamming with discrete subbands comparing to multisweep jamming with continual subbands is in the increased speed of jamming realization on necessary signal frequencies. In the case that sweep rate is the same in all three analyzed cases, the improvement factor in time duration (ITF_c) of one sweep cycle when sweep jamming with continual frequency subbands is applied towards pure sweep jamming is expressed as

$$ITF_c = \frac{f_{\max} - f_{\min}}{\sum_{i=1}^{n} f_{\max i} - f_{\min i}} \tag{3}$$

where it is:

- f_{max} and f_{min} – maximum and minimum swept frequency when pure sweep jamming is applied;
- f_{maxi} and f_{mini} – maximum and minimum swept frequency of the i^{th} subband when continual multisweeping is applied;
- n – number of subbands in the multisweep signal.

When multisweep jamming with discrete subbands is compared to multisweep jamming with continual subbands, the time ratio improvement (ITF_d) becomes:

$$ITF_d = \frac{\sum_{i=1}^{n} f_{\max i} - f_{\min i}}{\sum_{i=1}^{n}\sum_{j=1}^{m} f_{\max ij} - f_{\min ij}} \tag{4}$$

where it is:

- f_{maxij} and f_{minij} – maximum and minimum swept frequency of the j^{th} discrete subband as the part of i^{th} continual subband when continual multisweeping is applied;
- m – number of discrete subbands in each continual subband of a multisweep signal.

The effect of sweep time shrinking is especially important when very short messages are jammed, i.e. when jammed message duration is lower than one pure sweep period. Due to random message start time comparing to sweep signal realization, it is possible that jamming is not realized at all during the message time interval. But, when sweep jamming with continual subbands or sweep jamming with discrete subbands is realized, jamming could be surely achieved due to the decreased time of one sweep cycle.

The other possible action when short messages are jammed is to increase sweep rate instead to apply multisweep jamming with continual or discrete subbands. But, in this case jamming could be unreable because sweep rate is too high and the conincidence of drone signal frequency and jamming signal frequency is too short to cause secure jamming.

Performances of realized jamming signal

As it has already been stated, the most demanding requests for a drone jammer are related to the signal generation with the central frequency of 1200 MHz to jam drone communication and downlink video signals. The navigation signal channels are very near, with the central frequencies at 1176 MHz and 1227 MHz. In our system sweep signal is generated in a discrete subband between 1190 MHz and 1210 MHz.

It follows from [31] that it is necessary to jam frequency band about 1200 MHz in less than 10% situations. Although used less often for drone communication and video signal transmission than for other higher frequencies, the signals at 1200 MHz have several advantages, such as higher implementation range, higher reliability (less sensitivity to the influence of obstacles) and easier antenna construction. Signal transmission on the control link using frequency of 1200 MHz in the urban environment with lot of obstacles is investigated in [33]. Relatively rare implementation of 1200 MHz for drone communication and video signals transmission are the reason why it is very important and valuable to implement very reliable system for drones detection, identification and localization (DIL) together with a jammer. Precise identification allows us to determine which malicious drone model is applied. Such identification helps in the decision at what frequencies jamming has to be realized and whether it is necessary to perform jamming at 1200 MHz. As jamming of drone communication or telemetry signals at the frequency of 1200 MHz may easily become the reason for unwanted disruption of navigation signals in the jammer vicinity, it is necessary to avoid such jamming whenever it is possible. In other words, it is desirable to implement such jamming only when the malicious drone applies this frequency. It further means that the risk of unwanted navigation signals jamming exists in less than 10% situations when it is possible that the jammed drone applies this signal frequency.

Drone localization helps in the choice of jamming signal amplitude level. If malicious drone is near the jammer, the applied jamming signal amplitude level may be lower, thus avoiding undesired navigation signals disruption in a wide range. Contrary, if the detected malicious drone is at the great distance from the protected object, perhaps it will still not be necessary to jam its functioning until it comes nearer to the protected object. The great majority of solutions for drones DIL do not consider locating the drone operator, but such localization is also important [31]. If the drone operator was located nearer to the jammer than the malicious drone, it would be possible to disrupt downlink drone communication signals using lower jamming signal amplitude levels than in the case that this signal amplitude level is determined according to the drone position.

The Fourier transform of the generated jamming signal is calculated in Excel using its built-in Fourier Analysis tool in the Analysis ToolPack [34] and presented in Fig.3. The presented frequency charactristic is calculated with the frequency step of 1 MHz. The generated signal in the time domain may be expressed as:

$$s_0(t) = \sin(2 \cdot \pi \cdot (f_0 + \alpha \cdot t) \cdot t) \quad (5)$$

where f_0=1190MHz, α=20MHz/μs and 0≤t≤1μs. It now means that the sweep signal frequency is changed linearly between 1190 MHz and 1210 MHz as a function of time with the rate of 20 MHz/μs. The signal is generated during the time interval of 1μs. The attenuation at frequencies 1176 MHz and 1227 MHz is about 26 dB comparing to the signal level at 1200 MHz according to the characteristic in Fig.3. The typical sensitivity level at the input of telemetry receiver is -90 dBm (or, in some cases, -100 dBm) [35], [36]. If the power of generated jamming signal is adjusted in such a way that jamming signal level at the navigation signals receiver input is -90 dBm on the frequency 1200 MHz, the signal power level at the the same place on the frequencies 1176 MHz and 1227 MHz intended for satellite navigation is n_a=-116 dBm due to the attenuation 26 dB according to Fig.3. Therefore, taking into account the values from (1), this signal power level is between n_a-n_0=14 dB and n_a-n_1=44 dB higher than the threshold level of a satellite navigation signal receiver [32].

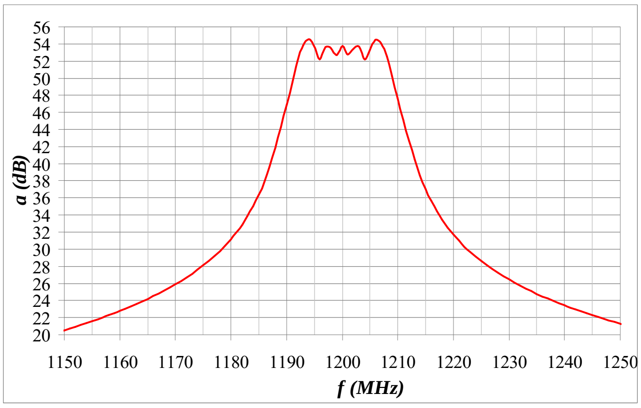


Figure 3. Frequency characteristic of a sweep jamming signal in a discrete subband between 1190 MHz and 1210 MHz

Let us calculate the spatial distance increase where jamming is disrupted comparing to the drone distance from a jammer. This calculation may be performed using Friis formula for the free space [37]:

$$\begin{aligned} P_R(dBm) &= P_T(dBm) + G_T(dB) + G_R(dB) \\ &-20 \cdot \log(r_{km}) - 20 \cdot \log(f_{MHz}) - 32.44 \end{aligned} \quad (6)$$

where P_T is transmitted signal power, P_R is the received signal power, G_T is the transmitting antenna gain, G_R is the receiving antenna gain, the constant 32.44 is intended to correct the use of units km for distance and MHz for frequency, r is distance between a jammer and a drone and f is system operational frequency. For our calculation G_T and G_R are 0 (they are not considered), P_T-P_R is between P_T-P_{R0}=-116dB-(-130dB)=14dB and P_T-P_{R1}=-116dB-(-160dB)=44dB (due to satellite navigation signals levels emphasized in (1)) and f=1200 MHz. Now it is obtained that r is between r=0.1m and r=3.15m. At 1176 MHz and 1217 MHz, according to Fig.3, these values without attenuation of 26 dB in a generated jamming signal frequency characteristic caused by the generated sweep jamming signal in the frequency range 1190 MHz – 1210 MHz would be r=2m and r=63m. Or, in other words, improvement when considering distance of undesired navigation signal jamming is 20 times (also follows from the attenuation of 26 dB at frequencies 1176 MHz and 1227 MHz comparing to attenuation at 1200 MHz according to 20·log(20)=26). The other important conclusion is that it is not necessary to take care of jamming navigation signals at 1176 MHz and 1227 MHz when it is necessary to realize jamming at 1200 MHz: jamming signal at 1200 MHz would successfuly jam also the two cited navigation signal frequencies. This is illustrated using Fig.4, which corresponds to Fig.3, but with signal levels at the y-axis adjusted to present the situation at the input to navigation signals receiver.

Let us suppose that signal power level of jamming signal at 1200 MHz is -90dBm (minimum level to cause successul telemetry signals jamming), as presented in Fig.4. According to the presented frequency characteristic, the jamming signal level at 1176 MHz and 1227 MHz would be about -116dBm as a consequence of the generated signal at 1200 MHz. This level is sufficiently higher than the expected level of navigation signals expressed by (1) to cause successful jamming.

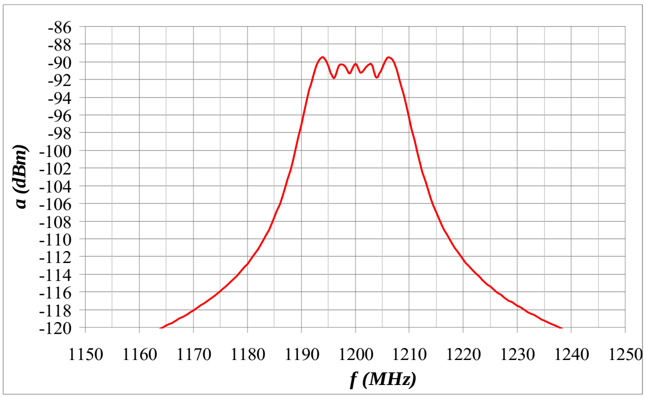


Figure 4. Frequency characteristic of a sweep jamming signal in a discrete subband between 1190 MHz and 1210 MHz – analysis for the jamming signal at the navigation signal receiver input

The second frequency range intended for navigation signals is between 1.57 MHz and 1.62 MHz. The jamming signal for this subband is presented in Fig.5. This signal is generated as a function:

$$s_1(t) = K_1 \cdot \sin(2 \cdot \pi \cdot (f_1 + \beta \cdot t) \cdot t) \quad (7)$$

where it is K_1=0.02, f_1=1550 MHz, β=5·α. The whole bandwidth between 1.57 MHz and 1.62 MHz is covered by only one discrete subband. The jamming signal amplitude level is about 40 dB lower than it is in the case of jamming communication and telemetry signals in Fig.3. The sweep rate is 5 times higher for Fig.5 (100 MHz/μs).

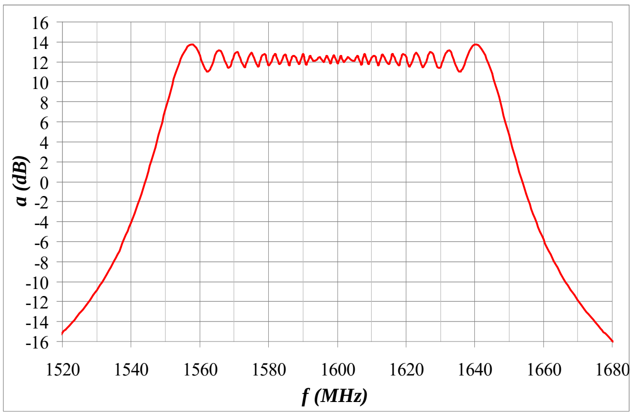


Figure 5. Frequency characteristic of a sweep jamming signal with one discrete subband in a frequency band between 1550 MHz and 1650 MHz

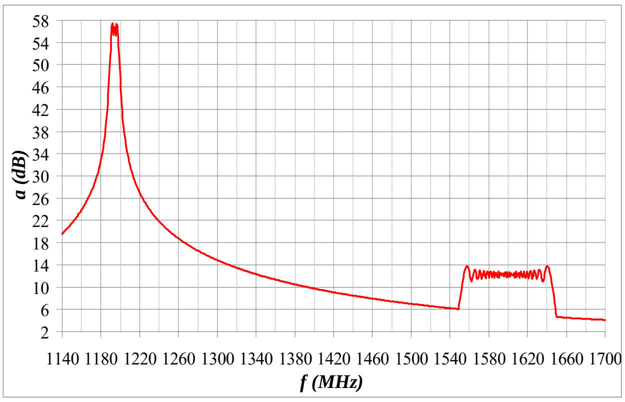


Figure 6. Frequency characteristic of a sweep jamming signal in two discrete subbands: a) between 1190 MHz and 1210 MHz and b) between 1555 MHz and 1645 MHz

Fig.6 presents jamming of communication and telemetry signal frequency 1200 MHz and navigation frequency band 1570-1620 MHz together (the figure is the fusion of characteristics from Figures 3 and 5, i.e. it presents a common effect of two jamming signals). In this case the frequency characteristic has attenuation higher than 48dB in the frequency band 1570-1620 MHz as a consequence of generated signal at 1200 MHz. This is illustrated by the frequency characteristic in Fig.7. In this graph the signal power level at 1200 MHz is about -90dBm and it falls to -138dBm at 1540 MHz and at even lower levels when the frequency is further increased. Such an attenuation level may not be enough to cause efficient jamming in all situations at 1570-1620 MHz. As a consequence, it is necessary to implement jamming in the frequency band 1570-1620 MHz in spite of jamming signal generation at 1200 MHz, which is illustrated in Fig.7 by the increased signal level to about -130dBm in this frequency range.

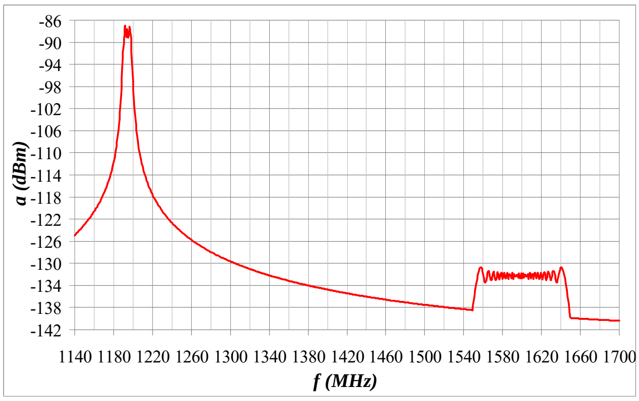


Figure 7. Frequency characteristic of a sweep jamming signal with two discrete subbands in a frequency band between 1550 MHz and 1650 MHz – analysis for the jamming signal at the navigation signal receiver input

Frequency band 1.57-1.62 GHz may be jammed using sweep signal with more frequency subbands. Fig.8 presents the case with two discrete subbands where the jamming signal is generated according to

$$s_2(t) = K_2 \cdot (\sin(2 \cdot \pi \cdot (f_{21} + \alpha \cdot t) \cdot t) + \\ + \sin(2 \cdot \pi \cdot (f_{22} + \alpha \cdot t) \cdot t)) \quad (8)$$

where K_2=0.15, f_{21}=1565 MHz, f_{22}=1605 MHz. The sweep rate for both presented subbands is α=20 MHz/μs.

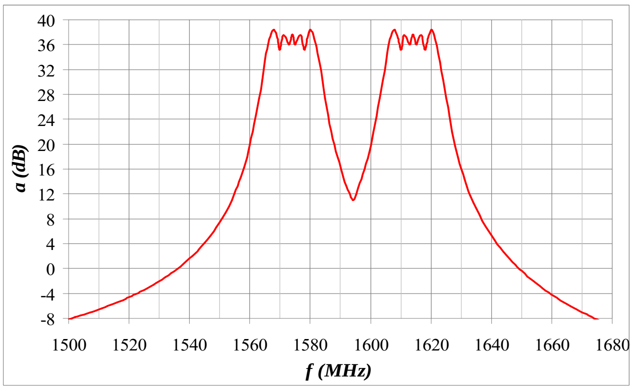
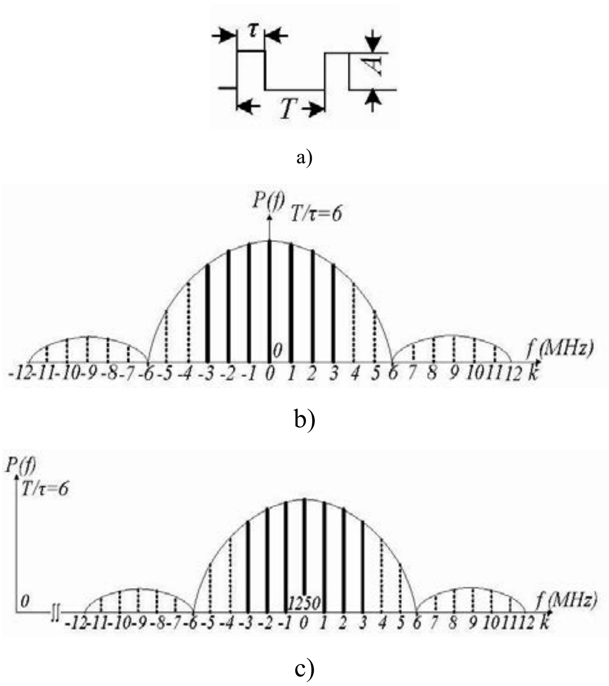


Figure 8. Frequency characteristic of a sweep jamming signal with two discrete subbands in a frequency band between 1550 MHz and 1650 MHz

Possibilities for method implementation for modern drone communication jamming

Today drone communication technologies and protocols are modernized with the aim to decrease jamming possibilities. Instead of classical communication protocols, modern drones may use Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS) protocol. Besides, techniques for jamming effect reduction are constantly developed and some such solutions are analyzed in [38, 39].

DSSS and FHSS use approximately the same frequency band included in the frequency range between 2.4 GHz and a bit less than 2.5 GHz for their function [40]. The number of the applied channels, the channel widths themselves and the frequency gap existence or non-existence for these two transmission methods are different. The transmission logic and algorithm for channels selection are also different. Nevertheless, it is necessary to implement constantly reliable jamming on a whole frequency band between 2.4 GHz and 2.5 GHz to prevent drone communication when it uses DSSS or FHSS.


τ
A
T
P(f)
T/τ=6
0
f (MHz)
-12-11-10-9-8-7-6-5-4-3-2-1 0 1 2 3 4 5 6 7 8 9 10 11 12 k
P(f)
T/τ=6
0
1250
f (MHz)
-12-11-10-9-8-7-6-5-4-3-2-1 0 1 2 3 4 5 6 7 8 9 10 11 12 k

a)

b)

c)

Figure 9. a) Rectangular pulse train signal in time domain; b) Power spectrum of rectangular pulse train signal; c) Power spectrum of frequency shifted rectangular pulse train signal.

Let us suppose that we have a rectangular pulse train signal of the amplitude A whose period is T and duration of each impulse is τ (Fig.9a)). The power spectrum of this signal is discrete and it is expressed as [41]:

$$P(f)=\sum_{k=-\infty}^{\infty}\frac{A^2\cdot\tau^2}{T^2}\cdot\frac{\sin^2\left(\frac{k\cdot\pi\cdot\tau}{T}\right)}{\left(\frac{k\cdot\pi\cdot\tau}{T}\right)^2}\cdot\delta\left(f-\frac{k}{T}\right) \tag{9}$$

where $\delta(f\text{-k}/T)$ is designation for places where discrete frequency components are situated and the remaining part in the equation presents frequency components power envelope. This power spectrum may be rich in frequency components in the range around f=0 Hz and it is presented in Fig.9b) for the ratio T/τ=6. Due to the spectral envelope in the shape of sin(x)/x, not all components in the main frequency lobe have enough signal level to cause jamming. Full lines in Fig.9b) present that seven of total 13 frequency components are used for jamming. The obtained frequency spectrum is further shifted to the frequncy range 2.4-2.5 GHz by the multiplication of the signal presented in Fig.9a) with the sinusoidal signal at the frequency 2.45 MHz. The obtained spectrum is presented in Fig.9c). The sinusoidal signal at 2.45 MHz may be additionally replaced by the multisweep signal with discrete subbands. The values of parameters A, τ, T as well as the parameters of multisweep signal, if it is applied, will be the subject of the further development.

Conclusions

In this paper, we have analyzed sweep jamming with discrete subbands, an advanced method for malicious drone jamming. This method allows us to realize jamming only in parts of frequency spectrum where it is expected that there are signals intended for operator mutual communication with drone, signals for drone navigation and video and telemetry data sending to the operator. It is possible to adjust jamming signal power level according to the characteristics of the implemented signals, which have to be jammed. The most demanding situation is the jamming of drone communication and telemetry signals when frequency 1200 MHz is used for these signals transmission, because two navigation signal frequencies 1176 MHz and 1227 MHz are in the near vicinity. Navigation signals have to be jammed for the considered hostile drone and not jammed for friendly systems as much as possible, which are two very opposed requests. The navigation signal receivers may detect these signals when their power level is even 40-70 dB lower than it is the detection threshold in the receiver of the communication and telemetry signals. Therefore, it is expected that navigation signals are disrupted on many friendly devices in a significantly wider area than it is necessary. Other implemented signal frequencies for communication, telemetry and video signals are more distant from navigation signals and there is significantly less risk to disrupt navigation signals on friendly systems because of communication, telemetry or video signals jamming.

The effect of unwanted navigation signal jamming may be decreased using the system for malicious drones' detection, identification and localization (DIL). The most effective way for drones DIL is implementation of artificial intelligence algorithms for the analysis of drone micro-Doppler signature figures obtained by radar sensor and this is going to be our further direction of development. Drone identification allows selecting the set of signal frequencies, which have to be jammed: for example, frequency 1200 MHz has to be jammed in less than 10% situations when a malicious drone is detected. Drone localization helps us to determine the drone distance from the jammer and it is possible to adjust the jamming signal power level according to this distance, thus decreasing the range around the jammer where navigation is disrupted.

References

[1] DENNING,L.: *Saudi Arabia Drone Attack is a Strike at Oil's Future*, Bloomberg, September 14th, 2019, https://www.bloomberg.com/opinion/articles/2019-09-14/saudi-arabia-drone-attack-is-a-strike-at-oil-s-future.

[2] RAZZOUK,N., BLAS,J., THORNHILL,J.: *Speed of Saudi Oil Recovery in Focus After Record Supply Loss*, Bloomberg, September 15th, 2019, https://www.bloomberg.com/news/articles/2019-09-15/saudis-race-to-restore-oil-output-after-crippling-aramco-attack.

[3] ERIKSSON,N.: *Conceptual study of a future drone detection system Countering a threat posed by a disruptive technology* , Master thesis in Product Development, Chalmers University of Technology, Goethenburg, Sweden, 2018.

[4] YAACOUB,J.P., NOURA,H., SALMAN,O., CHEBAB,A.: *Security analysis of drones systems: Attacks, limitations, and recommendations*, Internet of Things, Vol.11, pp.1-40, May 2020, https://doi.org/10.1016/j.iot.2020.100218.

[5] AARONIA drone detection: *AARTOS Anti-drone Jammers*, https://drone-detection-system.com/sensor-types-overview/anti-drone-jammer/?gclid=EAIaIQobChMI3pKNvuKm8wIVFtZ3Ch0hFgofEAAYASAAEgLQ5_D_BwE.

[6] AARONIA drone detection: *Sector Jammers PSJ360*, 2021

[7] SKYLOCK: *Effective, 360^o Antidrone Jamming System*, https://www.skylock1.com/anti-drone-jammers/rf-jamming-system/.

[8] RF Defence: *Portable Drone Jammer (with Built-in Battery)*, https://www.rf-defence.com/product/300w-portable-drone-jammer-with-built-in-battery.html?gclid=EAIaIQobChMI3pKNvuKm8wIVFtZ3Ch0hFgofEAAYBCAAEgKxU_D_BwE.

[9] MP2 technologies: *MAJES (Modular and Adjustable Jamming Efficient System*, https://www.mc2-technologies.com/1887-2/.

[10] MP2 technologoes: *Flyjam*, https://www.mc2-technologies.com/2834-2/.

[11] MATIĆ,V., KOSJER,V., LEBL,A., PAVIĆ,B., RADIVOJEVIĆ,J.: *Methods for Drone Detection and Jamming*, 10th International Conference on Information Society and Technology (ICIST), Kopaonik, March 8-11, 2020, In: Zdravković, M., Konjović, Z., Trajanović, M. (Eds.) ICIST 2020 Proceedings Vol.1, pp. 16-21, 2020.

[12] MILEUSNIĆ,M., PAVIĆ,B., MARINKOVIĆ-NEDELICKI,V,. PETROVIĆ,P., LEBL,A.: *Development, realization and testing the variant of the device for VIP persons protection in the extended frequency range (20MHz-6GHz) with the reduced total power (300W)*, tehničko rešenje – novi proizvod na projektu tehnološkog razvoja TR32051 "Razvoj i realizacija naredne generacije sistema, uređaja i softvera na bazi softverskog radija za radio i radarske mreže", 2017.

[13] MILEUSNIĆ,M., PAVIĆ,B., MARINKOVIĆ-NEDELICKI,V., PETROVIĆ,P., MITIĆ,D., LEBL,A.: *Analysis of Jamming Successfulness against RCIED Activation with the Emphasis on Sweep Jamming*, Facta Universitatis, Series: Electronics and Energetics, Vol.32, No.2, June 2019, pp.211-229, https://doi.org/10.2298/FUEE1902211M, extended and improved version of the paper awarded at 5th International Conference IcETRAN 2018, Palić, June 11-14, 2018.

[14] LEBL,A., MILEUSNIĆ,M., PAVIĆ,B., MARINKOVIĆ-NEDELICKI,V., PETROVIĆ,P.: *Programmable Generator of Pseudo-White Noise for Jamming Applications*, 27th Telecommunications Forum (TELFOR), Belgrade, November 26-27, 2019, Proceedings of Papers, pp.1-4, ISBN 978-1-7281-4790-1, DOI: 10.1109/TELFOR48224.2019.8971203.

[15] "IRITEL High Frequency (HF) radio surveillance and jamming system," in the book M. Streetly, "Jane's Radar And Electronic Warfare Systems," IHS Global Limited, 2011.

[16] "IRITEL Very/Ultra High Frequency (V/UHF) radio surveillance and jamming system," in the book M. Streetly, "Jane's Radar And Electronic Warfare Systems," IHS Global Limited, 2011.

[17] REMENSKI,N., PAVIĆ,B., PETROVIĆ,P., MILEUSNIĆ,M., MARINKOVIĆ-NEDELICKI,V.: *Integrisana radio-oprema za zaštitu prostora od mobilnih veza* (Treća generacija radio-opreme), tehničko

rešenje – novi proizvod s oznakom CJ-1P na projektu tehnološkog razvoja TR-11030 “Razvoj i realizacija nove generacije softvera, hardvera i usluga na bazi softverskog radija za namenske aplikacije”, 2010, http://www.iritel.com/images/pdf/cj-1p-e.pdf, (also published in the book M. Streetly, Jane’s Radar And Electronic Warfare Systems. IHS Global Limited, 2011). Prva generacija radio-opreme s oznakom CJ-1 je realizovana na projektu tehnološkog razvoja TR6149B, 2006.

[18] POKRAJAC,I., KOZIĆ,N., ČANČAREVIĆ,A., BRUSIN R.: *Jamming of GNSS Signals*, Scientific Technical Review, Vol. 68, No. 3, UDK: 621.396.96(047)=861, pp. 18-24, September 2018.

[19] PÄRLIN K.: *Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems*, Master’s Thesis, Tallinn University of Technology, Tallinn, 2017.

[20] PÄRLIN,K., ALAM,M.M., LE MOULLEC,Y.: *Jamming of UAV Remote Control Systems Using Software Defined Radio*, 2018 International Conference on Military Communications and Information Systems (ICMCIS), May 22nd-23rd, 2018, pp.1-6, Warsaw, Poland, DOI: 10.1109/ICMCIS.2018.8398711.

[21] FRIEDBERG,S.: *A Primer on Jamming, Spoofing and Electronic Interruption of a Drone*, April 19th, 2018, https://www.dedrone.com/blog/primer-jamming-spoofing-and-electronic-interruption-of-a-drone.

[22] SAARNISAARI,H.: *Sweep Jamming Hit Rate Analysis for Frequency Agile Communications*, 2016 International Conference on Military Communications and Information Systems (ICMCIS), May 23rd-24th, 2016, pp. 1-6, Brussels, Belgium, 10.1109/ICMCIS.2016.7496578.

[23] Drone Killer 6 – powerful UAV (GPS WIFI5GHz) Jammer – 120W, https://www.jammer-store.com/drone-killer-6.html.

[24] RADIVOJEVIĆ,J., LEBL,A., MILEUSNIĆ,M., VUJIĆ,A., ŠEVIĆ,T., JOKSIMOVIĆ,V.: *Multichannel Radio-jammer Development Considerations for prevention of Illicit Drone Missions*, 9th International Scientific Conference on Defensive Technologies OTEH 2020, Belgrade, October 15th-16th, 2020, pp. 270-275, ISBN 978-86-81123-83-6.

[25] RADIVOJEVIĆ,J., VUJIĆ,A., MILEUSNIĆ,M., PETROVIĆ,P., LEBL,A.: *Design problems in Implementation and Control of Malicious Drones Missions Jammers*, 8th International Conference IcETRAN 2021, Etno-Selo Stanišići, September 8th-9th, 2021.

[26] Homeland Security Science and Technology and National Urban Security Technology Laboratory NUSTL: *Counter-Unmanned Aircraft Systems*, Technology Guide (CUAS-T_G-1)”, September 2019.

[27] SHI,X., YANG,C., LIANG,C., SHI,Z., CHEN,J.: *Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges*, IEEE Communications Magazine, Vol.56, Issue 4, April 2018, pp.68-74., DOI: 10.1109/MCOM.2018.1700430.

[28] DROZD,A.L.: *Spectrum-secure Communications for Autonomous UAS/UAV Platforms*, MILCOM 2015 - IEEE Military Communications Conference, Tampa, Florida, October 26th-28th, 2015.

[29] *Drone Communication – Data Link: How do drones communicate with their operator?*, https://www.911security.com/learn/airspace-security/drone-fundamentals/drone-communication-data-link.

[30] SCHELLER,W.D.: *Detecting drones using machine learning*, thesis for master of science, Iowa State University, Ames, Iowa, USA, 2017.

[31] LIN,J.W.: *Civil UAV Monitoring Techniques*, The State Radio Monitoring Center.

[32] LOCOSYS Technology Inc: *Specifications for GPS receiver UC-1722*, March 2008.

[33] QIU,Z., CHU,X., CALVO-RAMIREZ,C., BRISO,C., YIN,X.: *Low Altitude UAV Air-to-Ground Channel Measurement and Modeling in Semiurban Enviroments*, Wireless Communications and Mobile Computing, Vol. 2017, Article ID 1587412, Hindawi, Wiley, pp.1-11, DOI: https://doi.org/10.1155/2017/1587412.

[34] “*How to evaluate a Fourier Series?*“, https://best-excel-tutorial.com/59-tips-and-tricks/334-fourier-series.

[35] Tualcom: *Telemetry Receiver*, September 2020.

[36] TR1013 Eagle Pro V2 1.2-1.3 GHz 500-1000mW Long Range Video Transmitter and Receiver Combo for FPV Air and Ground Applications, https://kazakhstan.desertcart.com/products/153481635-tr-1013-eagle-pro-v-2-1-2-1-3-g-hz-500-1000-m-w-long-range-video-transmitter-and-receiver-combo-for-fpv-air-and-ground-applications.

[37] GUSTAFSSON,J., HENRIKSSON,F.: *UAV Tracking Device using 2.4 GHz video Transmitter*, master’s thesis, Luleå University of Technology, 2005, ISSN: 1402-1617.

[38] NGUYEN,B.V., JUNG,H., KIM,K.: *On the Anti-jamming Performance of the NR-DCSK System*, Security and Communication Networks, Vol.2018, Article ID 7963641, pp.1-8, https://doi.org/10.1155/2018/7963641.

[39] TAMAZIN,M., KORENBERG,M.J., ELGHAMRAWY,H., NOURELDIN,A.: *GPS Swept Anti-Jamming Technique Based on Fast Orthogonal Search (FOS)*, Sensors 2021, Vol.21, Issue 11, 3706, May 2021, pp.1-15, https://doi.org/10.3390/s21113706.

[40] TANJUNG,H., AHMAD,N.B., ABDALLA,A.N.: *Spread Spectrum Processing Using Direct Sequence Spread Spectrum (DSSS) and Frequncy Hopping Spread Spectrum (FHSS)*, National Conference on Postgraduate Research (NCON-PGR) 2009, October 1st, 2009, UMP Conference Hall, Malaysia.

[41] BLACK,B.A.: *On the Generation of Waveforms Having Comb-Shaped Spectra*, NRL Memorandum Report 619, Naval research Laboratory, May 1988.

Received: 16.12.2021.
Accepted: 17.02.2022.

Ometanje prebrisavanjem sa diskretnim podopsezima – napredna strategija za sprečavanje dronova korišćenih u zlonamerne svrhe

Ometanje dronova korišćenih u zlonamerne svrhe je predmet brojnih istraživanja u svetu. Primenjene strategije ometanja su različite u pojedinim slučajevima i svako unapređenje u analizi, modelovanju i realizaciji doprinosi originalnosti u procedurama ometanja. U ovom radu analiziraju se karakteristike ometanja prebrisavanjem sa diskretnim frekvencijskim podopsezima. Ova napredna metoda omogućava da se smanje problemi izazvani ometanjem komunikacionih i/ili telemetrijskih signala koje koriste dronovi na neželjen poremećaj navigacionih signala (GPS i GLONASS) korišćenih za lokalizaciju dobronamerno korišćenih uređaja u blizini ometanog drona. Problem je analiziran na primeru jedne signalizacione frekvencije namenjene zakomunikaciju između drona i operatora. Dronovi sa ovom specifičnom signalizacionom frekvencijom koriste se relativno retkko, ali su dobijeni rezultati vrlo ilustrativni za praktičnu analizu problema. Specifičnost ove frekvencije je da je ona najbliža frekvencijama navigacionih signala što znači da se važni zaključci u odnosu na ovu frekvenciju neuporedivo lakše zadovoljavaju kada su u pitanju druge frekvencije namenjene za slanje komunikacionih, video i telemetrijskih signala dronova.

Ključne reči: **zlonamerno korišćeni dronovi, ometanje prebrisavanjem, diskretni podopsezi, komunikacioni i telemetrijski signali, navigacioni signali.**