Russian Wireless and Mobile Jammers: Efficiency Comparison

Sergey Rybalkin
Saint Petersburg State University of Aerospace Instrumentation (SUAI)
Saint Petersburg, Russia
e1720@yahoo.com

Anton Sergeev
Saint Petersburg State University of Aerospace Instrumentation (SUAI)
Saint Petersburg, Russia
slaros@vu.spb.ru

***Abstract*— Radio jamming in wireless and mobile networks is a topical research problem due to the ease in blocking wireless communications. In this work, we provide analytical and experimental comparison of popular Russian radio jammers by the criterion of blocking efficiency of wireless/mobile signals. The level of electromagnetic noise (dB/mcV) was estimated experimentally for different wireless systems and for different jammers. Experiments were focused mostly on jamming WiFi and 3G communications. The experimental results show that some jammers do not really block wireless signals completely.**

I. JAMMING OF WIRELESS COMMUNICATIONS

A radio jammer is a device used to deliberately prevent authorized or non-authorized wireless communications. They are used to block information flow in wireless and mobile networks due to security reasons. The typical scenarios for legal usage of radio jammers usually include:

- guarantying of confidentiality of communicated data and disabling non-authorized access to communications (mobile/wireless bugs) during the business, military or political negotiations by jamming the selected radio channels;
- permanent blocking of mobile communications (cell phones of legal visitors) at protected objects (e.g. in consulates, military bases);
- temporary blocking of all wireless signals at a secured area during the important event to (e.g. at school exams);
- temporary blocking of remote radio detonators;

Attackers can also apply jamming for denial-of-service (DoS) attacks to make a machine or network resource unavailable to its intended users. This could be very dangerous due to prevalence of new wireless applications, and devices. One of interesting cases are medical implants, where wireless access to the implant data is safety-critical and must be granted to medical professionals in all circumstances. Hackers can use radio jamming in this case to block legal access to the medical equipment or even for doing direct damage to human health and lives.

In all these cases it's very important or even critical to understand the real potentials and efficiency of radio jammers in practice and have benchmarks in real environment.

The goal of this paper is to analyze efficiency of popular Russian jammers by the criterion of blocking different mobile and wireless communications. The key questions of the research are: "Does radio jammers really block all the wireless and mobile communications?"; "What communication standards are supported and what radio systems can be suppressed?". The results of the work can be used in designing, enhancing and testing anti-jamming techniques [1],[4].

The related works concentrate mostly on jamming and anti-jamming methods, theoretical comparison and modeling [2]. Some practical scenarios and limitations of radio jamming can be found in [3]. Problems of error correction and modulation in wireless transmission caused by jamming are considered in [4].

II. OVERVIEW OF RUSSIAN RADIO JAMMERS

The following popular radio jammers are analyzed and compared in this paper:

- BugHunter Black P24 [5]
- LGS-715 [6]
- ST 202 UDAV-M [7]
- Scorpion 200 [8]

All the listed models are recommended by Russian authorities and regulators to provide information security and preventing leakage of protected data.

A. BugHunter Black P24

BugHunter (see Fig. 1) is a stationary indoor/outdoor radio signal jammer for mobile communication systems working in 6 frequency ranges:

- 4G MOB: 780-830 MHz
- GSM900: 925-960 MHz
- GSM1800: 1805-1880 MHz
- 3G: 2110-2170 MHz
- 4G: 2620-2690 MHz

It blocks operation of GSM bugs, cell phones, data transfer, Internet access. It's focused on blocking mobile (cellular) communications and does not suppress WLAN/WPAN networks (for example, WiFi).

of medical implants, where access to the implant data is safety-critical and must be granted to medical professionals in all circumstances.

ISSN 2305-7254

Fig. 1. Radio Jammer Bug Hunter P24

B. *LGS-715*

The signal cellular network radio suppressor (jammer) LGS-715 (Fig. 2) is intended for blocking devices operation of unauthorized obtaining information working in standards of cellular networks, Bluetooth and WiFi.

In contrast to BugHunter the list of blocked wireless standards does not include LTE (4G), but IMT-MC-450 and AMPS are added instead.

Fig. 2. Radio Jammer LGS-715

The principle of operation consists in noise generation in the several frequencies ranges:

- IMT-MC-450: 462,5-475 MHz
- AMPS/DAMPS800: 869-894 MHz
- GSM900: 935-960 MHz
- DSC/GSM1800: 1805-1900 MHz
- IMT-2000/UMTS (3G) 1: 2010-2025 MHz
- IMT-2000/UMTS (3G) 2: 2125-2170 MHz

One of the key features of the device is that the smooth power control of interfering signal in each of the ranges is possible. It allows to block wireless standards of communication only within the security perimeter (protected location).

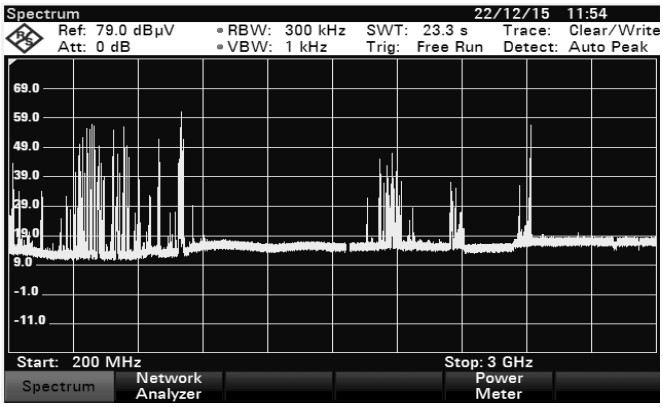

Fig. 3. Frequency range for LGS-715: 200MHz-3GHz

Fig. 4. Radio Jammer ST 202 UDAV-M

C. *Jammer ST 202 UDAV-M*

ST 202 UDAV-M is intended for support information security talks by blocking wireless communications which can be used for unauthorized data transmission by bugging devices within the secure working zone. There is a power control possibility on each suppression channel. UDAV-M has the longest list of jammed communication systems:

- CDMA450
- GSM900
- GSM1800
- WI-FI
- Bluetooth
- 3G
- 3G low
- WiMax (4G)
- LTE800

It also has a very useful feature of automatic detection of wireless devices. When the radio signal is detected than jamming signal is enabled on the corresponding channel.

D. *Jammer Scorpion 200*

The devices blocks 5 channels: GSM - 900/1800, CDMA - 800, 3G – 2100, 4G LTE (4G), WIMAX (technical specifications has no detailed information regarding frequency ranges). Scorpion 200 includes infrared remote control.

III. Experimental equipment

In the experimental campaign we used radio spectrum analyzer Rohde & Schwarz FSW8 for measurements and efficiency estimation of the jamming signal (electromagnetic interferences), generated by the compared devices. Technical specifications of the spectrum analyzer can be found on the official website of the vendor [9].

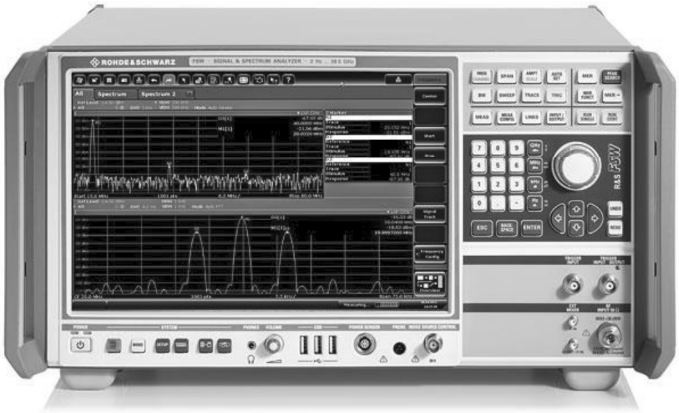

Fig. 5. Radio Spectrum analyzer Rohde & Schwarz FSW8

The experiment took into account device parameters such as frequency range, measurement accuracy, bandwidth, and phase noise. Phase noise is only shown on the display if the displayed signal is strong enough to rise above the level of system noise.

The list of tested frequency ranges includes:

- 3G-Uplink 1920-1980 MHz
- 3G-Downlink 2110-2170 MHz
- WiFi 2400-2483,5 MHz
- Bluetooth 2402-2480 MHz

III. Results of Experiments

1) Bug Hunter: The signal form changes when the jammer is turned on. Please note a significant increase of dB/mcV value from 54.8 to 72.7.

However, the unstable level of suppression is detected. It may be explained by the insufficient range of suppression and level of electromagnetic noise. Experiments with the 3G and LTE frequencies showed a complete blocking of a signal.

2) LGS-715. The results of signal jamming are shown on the pictures 6-10 The experiments shows that LGS-715 can perfectly block WiFi and GSM.

Fig. 8-9 shows that jamming of 3G/UMTS does not work correctly. When enabled LGS-715 increases level of electromagnetic noise for 3G channel from 40.9 to 41 dB/mcV only. One can see that 3G/UMTS is not blocked. That was confirmed by the fact that more than 88% of incoming SMS can be received by cell phones, located within the jammed area.

3) ST 202 UDAV-M. Experimental results for ST 202 for the frequencies of 3G DownLink (2130 – 2170 MHz) show that the level of electromagnetic noise generated by the device is quite enough to effectively blocks all the wireless signals.

We also tested ST 202 as a detector of wireless devices with the subsequent automatic turning on a jamming signal on the selected channel. In our tests mobile call at the smartphone (distance 1m, 3m, 5m, 10m) was detected. That immediately enabled full suppression of 3G signal. The measurement shows that dB/mcV sharply increases from 20.2 to 65.3.

4) Scorpion 200. The jammer effectively blocks all the channels in all operation modes. Suppression of 3G UpLink (1920-1980 MHz) signal is very stable. When jammer is enabled, the level of electromagnetic noise is increased and exceeded background level: value of dB/mcV increases from 16.9 to 48.2.

II. Conclusion

Table I presents key technical parameters and summarizes experimental results for the compared radio jammers. One can see that ST 202 UDAV-M is the most powerful solution, which can effectively block almost all wireless and mobile communication systems indeed. It's also the most expensive one but it's worth it.

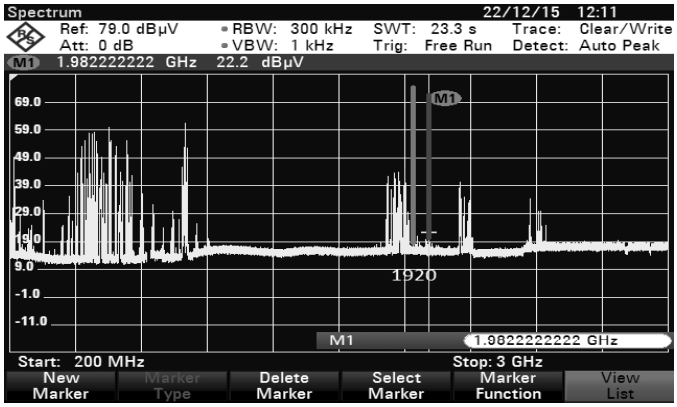

Fig. 6. Uplink 3G: LGS-715 Jammer is switched off

Fig. 7. Uplink 3G: LGS-715 Jammer is switched on

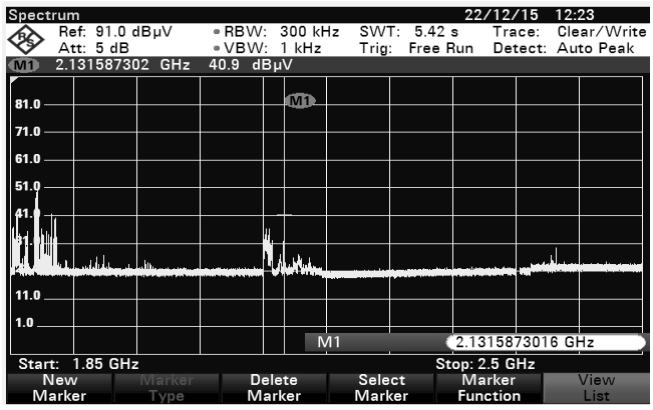

Fig. 8. Downlink 3G (2110-2170 MHz): LGS-715 Jammer is switched off (increased scale for 1.85 GHz)

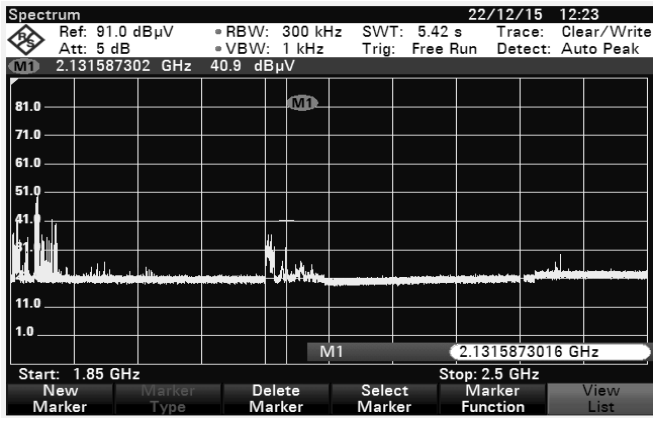

Fig. 9. Downlink 3G (2110-2170 MHz): LGS-715 Jammer is switched on (increased scale for 1.85 GHz)

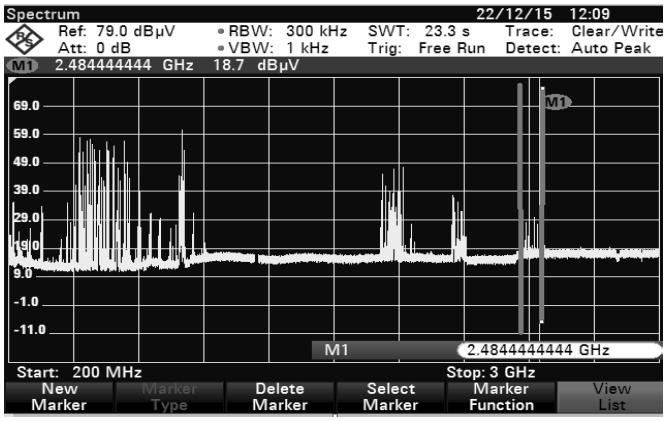

Fig 10. WiFi 2400-2483,5 MHz. LGS-715 Jammer is switched off

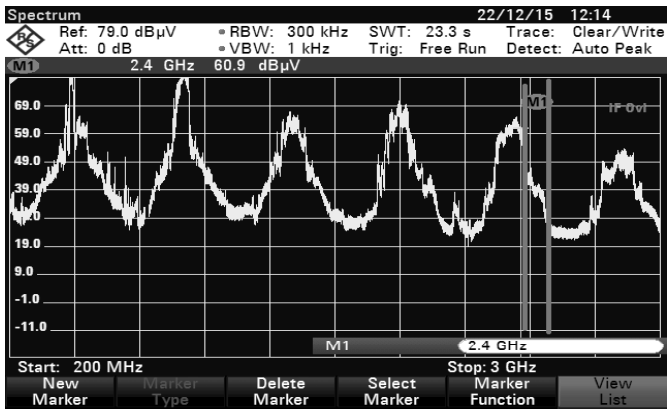

Fig 11. WiFi 2400-2483,5 MHz. LGS-715 Jammer is switched on

TABLE I. COMPARISON OF WIRELESS AND MOBILE SIGNAL JAMMERS

Jammer/Parameter	BugHunter	LGS 715	ST 202 UDAV	Scorpion 200*
Wireless Communication Standards				
IMT-MC-450, MHz	450-470	462,5-475	462,5-467,5	
4G MOB	780-830			
AMPS/DAMPS800, MHz	869-960	869-894	869-894	
GSM900, MHz	925-960	935-960	925-960	+
DSC/GSM1800, MHz	1805-1880	1805-1900	1805-1900	+
3G Uplink, MHz	2110-2170 **(blocking unstable!)**	2010-2025	2110-2180	+
3G Downlink, MHz		2125-2170 **(blocking failed!)**		+
4G	2620-2690			+
WIFI, MHz	-	2400 - 2483,5	2400-2484	
Bluetooth, MHz	-	2402 - 2480	2402 - 2480	
Parameters				
Max Jamming Distance, m	40	40	40	45
Remote Control	-	-	Yes	Yes
Channel Selection	Yes	Yes	Yes	-
Selection level of jamming signal	Yes	Yes	Yes	-
Price, $	150	1000	1100	120

LGS-715 jammer is very similar to a previous one and has a similar set of features. Unfortunately our tests demonstrated that LGS-715 fails in blocking 3G Downlink and signal could be delivered when the jammer is switched on.

BugHunter and Scorpion are cheap low-end jammers. The noise level is quite unstable. Anyway in all our experiments tested channels were blocked. It should be added that BugHunter has very impressive functionality compared to hi-end models (channel and level selection, 6 frequency ranges etc.) at a very low price.

We hope that our work will help developers and researcher in mobile and wireless communications. Right now we are planning to apply the obtained results in our research activities in wireless video transmission, run practical tests with jamming (e.g. to make a series of field experiments of new source-channel coding scheme for video transmission [10],[11]).

REFERENCES

[1] Roger Piqueras Jover, Joshua Lackey, Arvind Raghavan, *Enhancing the security of LTE networks against jamming attacks*, EURASIP Journal on Information Security, DOI: 10.1186/1687-417X-2014-7

[2] Kanika Grover et al, *Jamming and anti-jamming techniques in wireless networks: a survey*, International Journal of Ad Hoc and Ubiquitous Computing, 2014

[3] Nils Ole Tippenhauer, Luka Malisa, Aanjhan Ranganathan, Srdjan Capkun, *On Limitations of Friendly Jamming for Confidentiality*, Security and Privacy (SP), 2013 IEEE Symposium on, DOI: 10.1109/SP.2013.21, 2013

[4] Evgenii Krouk, Sergei Semenov, *Modulation and coding techniques in wireless communications*, John Wiley & Sons, 2011 [5] Radio Jammer BugHunter Black P24, Web: http:// www.bughunter.ru/podavitel-sotovyh-telefonov-baghanter-black-p24.php

[6] Radio Jammer LGS-715, Web: http://www.pps.rupart =catalog&product=82

[7] Radio Jammer ST-202M Udav-M,Web: http://www.blackhunter.ru/ shop/item/44

[8] Radio Jammer Scorpion 200,Web: http://www.aurix.ru/ product_150.html

[9] Analyzer Rohde & Schwarz FSW8, Web: www.rohde-schwarz.ru/products/test_and_measurement/spectrum_ analysis/FSW

[10] A.Sergeev, A. Turlikov, A.Veselov, *Joint Source Coding and Modulation for Low-Complexity Video Transmission*, XII International Symposium on Problems of Redundancy in Information and Control Systems, pp. 33-41, 2009

[11] A. Sergeev, A. Turlikov, A. Veselov, *Statistical Modulation for Low-Complexity Video Transmission*, The 11th International Symposium on Wireless Personal Multimedia Communications, Finland, 2008