

RF Jammer Testing Report for uWatch



Assured Service Provider



Cyber Advisor (Cyber Essentials)

March 14 2024



Executive Summary

The UK is experiencing a rapid increase in the use of 'Jammers' by criminals in order to evade a variety of security products and services. The current use of Jammers prevents two way communication from Wi-Fi, 3g, 4g, 5g, GPS, and many other forms of communication protocols, thus enabling the criminals to gain access and steal farm machinery, Cars and Vans, livestock, etc. by either evading wireless communication security mechanisms and/or preventing phone and internet connection to raise the alarm. This has also been adapted to enable organised shop lifting in large shopping centres and stores the disruption of WiFi based retail systems.

The increasing use of Wi-Fi enable CCTV, IP Telephony, credit card terminal communication, Wi-fi enabled Intruder Alarms continues to develop with the introduction of IoT and OT Wi-Fi communication adoption.

uWatch approached 10Steps Ltd to perform a series of independent test to establish the effectiveness of the their 'Cube' product to communicate securely and continuously in the presence of multi-frequency RF Jammers and therefore enable communication and photo transfer to external receivers which may be based up to 7km away (clear line of sight) using an adapted LoRa protocol.

Testing Process

A multi frequency Jammer was provided by a police force for the testing, with the same model being readily available off the internet from:

*[<http://www.onbuy.com>]www.onbuy.com and www.Fruugo.com for under £300.
https://www.fruugo.co.uk/10-band-gps-signal-2g3g4g5ggpsbeidouwifi-camera-finder-no-gps-positioning-tracking-eu-plug-k13/p-272700436-604843309?language=en&ac=croud&asc=pmax&gad_source=1*

A 'Cube' (a 4cm square cube – Serial No:1061, powered internally by batteries) and a "flat Cube" base station. (powered by USB C cable) were provided by uWatch.

Remote sensors known as "LoRa! Tags were used to activate the devices at various ranges.

The 'Cubes' were triggered via the Tag from a variety of locations and conditions (behind objects, trees, buildings, etc.) at a variety of distances up to 75m. Timing was performed at various point of the day and night to provide varied frequency traffic from Mobile Devices and Wi-Fi use to ensure that the tests were both fair and 'real life'.

Testing Results

Cube Distance from Receiver	Recorded Signal Strength	Jammer Enabled	Pass/Fail
1 meter	75%	NO	PASS
1 meter	69%	YES	PASS
10 meters	75%	No	PASS
10 meters	68%	YES	PASS
25 meters	57%	NO	PASS
25 meters	41%	YES	PASS
50 meters	58%	NO	PASS
50 meters	41%	YES	PASS
75 meters	47%	NO	PASS
75 meters	41%	YES	PASS

Conclusion

Testing concluded that the 'Cube' device did consistently communicate to the base station while in the presence of an active jammer. uWatch were not present during the testing and did not provide any information regarding setup and use, other than the standard information sheet found in the box.

Testing was repeated at various times to ensure increased mobile and Wi-Fi traffic did not affect the results, the weather was conducted in moderate wind conditions both in the dry, and in light rain conditions.

Due to the nature and impact of the 'Jammer' tests were cut to the minimum of time, typically 30 seconds and could not be tested over a long period of continuous time, however it was also recorded that all Wi-fi and mobile communications were disabled on every available device within the 25m claimed range of the jammer proving the scope and effectiveness of the signal Jammer itself.

Note: The technology used to develop a device which can work effectively in an environment alongside a jammer is considered a trade secret.

Jason Cresswell
 CEO and Founder
 10Steps Ltd
 07367 599500

